THE NATIONAL SUPERVISORY AUTHORITY FOR PERSONAL DATA PROCESSING

ANNUAL REPORT

2013

The activity report is presented to the Senate of Romania, in virtue of Article 5, Law no. 102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing, with further changes and amendments.

Bucharest

FOREWORD

Mr. President of the Senate,

Esteemed Senators,

I bring to your attention the report on the activity of the National Supervisory Authority for Personal Data Processing for 2013, following my appointment as President on the 26th of June 2013.

In the first year of the mandate as President of this important institution for the protection of fundamental rights in Romania, our activity was focused on ensuring an optimal performance of legal duties, monitoring and control of the processing of personal data under the jurisdiction of the Authority.

Thus, the main coordinates of the work carried out during the year 2013 aimed to: intensify the control actions of the legality of data processing, approval of draft regulatory acts with relevance in this field and active participation in the process of reform of the legislation on protection of personal data in the European Union and the European Council.

The Authority's involvement in the reform process of the European regulations concerning the processing of personal data, triggered in 2012, has been enhanced, in order to ensure a meaningful position within European system, in collaboration with other public institutions in Romania, with the role of representation at this level.

In the second part of the year, our institution's efforts were focused on increasing the intensity of the control actions carried out to solve the complaints and notices received, and also for the verification of certain aspects of the processing of personal data, in order to ensure compliance with and application of the principles of data protection by data controllers in the public and private sector. The investigations aimed, in particular, the work done in the banking and finance sector, electronic communications and on-line environment, as well as in that of monitoring and security of the public or private areas through the use of means of video surveillance. The result of this approach was an increase of over 300% of the amount of the fines applied in 2013, compared with the previous year and also a significantly increase of the number of complaints and notices

addressed by those interested.

Based on the experience gained this year, we propose that one of the objectives of the Authority's strategy on short and medium term will aim to increase the public awareness of all the entities involved and of the data subjects of particular significance with regard to respecting the right to protection of personal data, as well as awareness of the consequences that may occur in the event of breaching it, by applying coercive measures.

For this purpose, however, it is necessary to strengthen the administrative capacity of the National Supervisory Authority for Personal Data Processing through the allocation of material, human and financial resources corresponding to its specific duties, in accordance with the standards required by European legislation. This way, the institution will be prepared for fundamental changes from a legislative and operational point of view which will involve the adoption of the reform package at the level of European organisations to which Romania is a part of.

I express my belief that we will have the support of all decision-makers for future projects of this independent authority, to be able to carry out the role of guarantee of the actual protection of right to privacy and the right to protection of personal data.

Ancuța Gianina OPRE,

President

Table of Contents

CHAPTER I

OVERVIEW……..……..…..6

CHAPTER II

EUROPEAN UNION LEGILATIVE PROCEDURES

Section 1 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data and the Proposal for a Directive on the protection of the data processed for the purpose of prevention, investigation, detection and prosecution of criminal offenses under implementation and other judiciary activities**……..……..8**

Section 2 Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union and Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme**……..…..…11**

Section 3 Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a Proposal for a Regulation of the European Parliament and Council on information accompanying transfers of funds**…….……..…14**

CHAPTER III

REGULATORY ACTIVITY, ADVISING, CONSULTATION AND PUBLIC INFORMATION

Part 1 Approval of legislative acts …….....…...17

Part 2 Opinions on various aspects of data protection …….....…..28

Part 3 The representation activity before courts of law……..... 44

Part 4 Public information …….....….....48

CHAPTER IV

THE CONTROL ACTIVITY

Section 1 Overview …….....49

Section 2 Ex officio investigations …… 51

Section 3 The activity of solving complaints and notices ……..…….....62

CHAPTER V

INTERNATIONAL RELATIONS' ACTIVITIES ……..... 81

CHAPTER VI

PERSONAL DATA PROCESSING SUPERVISION ACTIVITY

Section 1 The activity of data processing registration …….....85

Section 2 The transfer of personal data .....…….....88

CHAPTER VII

THE ECONOMIC MANAGEMENT OF THE AUTHORITY …….....90

CHAPTER I
OVERVIEW

The National Supervisory Authority for Personal Data Processing activity report for 2013 is structured on seven chapters, as follows:

Chapter I presents the report's structure according to the main issues.

Chapter II shows the relevant aspects of the initiatives having an impact on the personal data protection field on the European Union level.

Chapter III shows the activity in the field of regulation, advising and consultation, especially the approval of legislative proposals concerning issues of data protection and the clarification of the problems raised by various data controller. This was materialized in the issuing of 32 approvals and 625 points of view.

Through the petitions addressed to the authority, the natural persons and the data controllers have asked for information about incidence of the legislation regarding data protection on the data controllers' activity, the processing of sensitive data, the legality of disclosing certain data, their transfer abroad.

In the section about the representation before courts of law are presented the relevant litigations to which the National Supervisory Authority for Personal Data Processing (named from here on the National Supervisory Authority) was a part of and the given resolutions are underlined.

The section concerning public information shows the main methods of popularising the personal data protection field, used by our institution.

Chapter IV consists of a presentation of the control activity, concerning the ex officio investigations and those carried out based on the complaints or notices received. This activity consists in checking the ways in which the Romanian data controllers carry out personal data processing operations with the aim of knowing how the legal dispositions of the field are applied in practice. Following these investigations, contravention sanctions were applied consisting in warnings and fines in total of 134,500 lei.

The ex officio investigations focused on the compliance of the data controllers with the provisions of Law no. 677/2001, as well as of other legislative acts concerning the personal data field.

In some cases, the President of the National Supervisory Authority has decided to end processing operations or to delete the processed data.

Chapter V shows the National Supervisory Authority's foreign relations activity.

Chapter VI, on personal data processing supervisory activity, shows the conclusions drawn from analyzing the forms sent by the data controllers, natural and legal persons that had the obligations to send them. A total of 7499 notifications about data processing both in Romania and in other member states, or transfers to third states, have been registered.

Chapter VII, about material and financial means, contains information regarding budgetary credits at the disposal of the National Supervisory Authority and the sums spent on every article in the budgetary classification.

CHAPTER II
EUROPEAN UNION'S LEGILATIVE INITIATIVES

Section 1: A Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data and the Proposal for a Directive on the protection of the data processed for the purpose of prevention, investigation, detection and prosecution of criminal offenses under implementation and other judiciary activities

The legislative package proposed by the European Commission contains two regulatory documents proposals:

- a proposal for a Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data;
- a proposal for a Directive on the protection of data processed for the purpose of prevention, investigation, detection and prosecution of criminal offenses under implementation and other judiciary activities

Basically, Romania endorses the adoption of the new legislative package relating to data protection, in order to ensure the effective and uniform protection of the right to privacy at European Union level. The National Supervisory Authority has already declared its support for the consolidation of the rights of individuals, whose personal data are used in the public and private sector, including the institution of new rights, which are the right to be forgotten and the right to data portability, in accordance with the modern day technological evolutions.

Concerning the nature of the juridical instrument, the European Commission has proposed a regulation, a directly applicable regulatory act, with the declared intention to ensure a regulation and approach unity towards personal data protection at the European Union level.

In the context of the debates within the DAPIX Working Group at the level of the European Union Commission, one aspect noted by many member states was that of the high number of delegated and implementing acts that would be issued by the European Commission, in order to put the regulation into practice. Following these debates, the cases in which the Commission would approve such acts were few, the member states opting for terminally deletion of the delegated acts or expressing their

agreement to replace the delegated act having practical provisions in the body of the regulation proposal.

About raising the number of the data controllers' administrative tasks, especially concerning micro-enterprises and small and medium enterprises, Romania has noted that their obligations and costs will rise, and the majority of member states have endorsed the introduction of an approach based on the risks implied by certain data processing.

A novelty is the introduction of the obligation of the data controllers to notify the National Supervisory Authorities about any breach of the conditions of security of data processing. In this respect, the National Supervisory Authority has alleged that the notification should be done only in case of important personal data security breach, when it can affect the natural persons. Because of this aspect, it has been brought upon the data controllers the obligation to also inform the natural persons whose data are involved in the security breach notified to the supervisory authorities. In this respect, the National Supervisory Authority thinks that it should be left up to these authorities to decide if the data subjects' information is required, in order to avoid alarming them in minor situations, maybe even already solved by the data controller.

Another important aspect is that referring to the appointment of the National Supervisory Authority's management, as to which Romania has argued that it should be done exclusively by the Parliament, so that it will have a real independent status.

Another proposed provision is about the transmission of the National Data Protection Authority's decision drafts to the European Data Protection Board and the European Commission, in certain cases, a situation that could affect the National Data Protection Authority's independence in its relation with the European Union's executive.

Another proposal over which there were numerous talks refers to the conditions for appointing a Data Protection Officer at the level of data controllers.

The chapter concerning the ways to undertake personal data transfers has raised big interest, and the "lead-authorities" mechanism proposed by the European Commission has been widely discussed, underlining the positive aspect, but also the negative implications from the person that is directly affected by the point of view.

As for the proposal for a Directive on the protection of data processed for the purpose of prevention, investigation, detection and prosecution of criminal offenses under implementation and other judiciary activities, the European Commission has underlined that its aim is to ensure a unitary and high level of personal data protection for the natural persons in the field of police cooperation and for the legal persons in criminal matters. Therefore, it is meant that the level of protection for natural persons'

rights and liberties concerning personal data processing by the competent authorities, with the aim to prevent, identify, investigate and prosecute crimes and carry out sentences, to be similar in all other member states.

The actual personal data protection at the European Union level implies the personal data subject rights consolidation and the consolidation of obligations for those who process personal data, as well as assessing the equivalent competency for monitoring and ensuring the conformity with the personal data protection regulations in member states.

Consequently, the proposal's aim is to ensure a high level of data protection in this field, thus augmenting mutual trust between the police and the judiciary authorities from various member states, easing the free movement of data and the cooperation between these authorities.

About this proposal, the National Supervisory Authority has formulated certain reservations regarding the extension of applicability domain of Directive concerning the activity of maintaining and assuring public order, because the derogatory regime from the observing the person's rights, as well as for the activities in the criminal law field, is not justified in the public order, also.

During the debates conducted in the Dapix Working Group at the level of the European Union Council, a strong accent has been laid on the regulation of the data subject's rights, with reference to the exigency to establish an adequate level of personal data protection and by Directive proposal.

This legislative package is in the debate phase at European Union Council level.

Section 2: Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union and Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme (RTP)

On the 28th of February 2013, the European Commission has launched a new legislative package, titled **"Smart Borders"**, which comprises the following initiatives:

1. **Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union**

The purpose of constituting a system of Entry/Exist (EES) to register data about the entry and exit of third country nationals crossing the external borders of the Member States of the European Union is to improve the management of the external border and the fight against irregular migration, by

providing a system that will:

- calculate the authorized stay of each traveller,
- assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, or stay on the territory of the Member States; this concerns notably persons who are found during checks within the territory not in possession of their travel documents or any other means of identification,
- support the analysis of the entries and exits of third-country nationals.

The Entry/Exit System (EES) will not apply to third parties family members of European Union citizens, in possession of a residence permit or to the owners of residence permits, which are mentioned in the Schengen Borders Code, because their residency is not limited to 90 days during a 180 day period.

2. Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme (RTP)

The objective of the Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme (RTP) is to:

- establish the procedures and conditions for access to RTP,
- determine the purpose, functionalities and responsibilities for a token—Central Repository as a data storage system about registered travellers,
- to confer to the IT Agency (EU—LISA) the operational management and development of the Central Repository.

The aforementioned Proposal for a Regulation also defines the procedures and conditions for submitting an access request to RTP, the examination procedures of said requests and decision making concerning them, the administrative management and system organization, the technical architecture of the token system—the central repository, the data categories and data entry by the competent authorities, the data usage method, the period of retention, data modification, data subject's rights and the supervision of the legality of personal data processing.

Considering the proposals contained within the "Smart Borders" legislative package, the National Supervisory Authority assessed that the implementation of a data collection and processing system through the European entry/exist system and the registered traveller program assumes a large scale processing of personal data and can be a new risk for personal data protection of natural persons and, consequently, respect for and safeguarding of their fundamental rights, especially the right to privacy.

Such a system that can ensure a rapid access to informational control systems and entry/exist inventory at European Union border, as well as authorized biometric data control, is based on the processing of various personal data categories, especially the sensitive ones (biometrics).

The National Supervisory Authority has underlined that the above-mentioned activities, developed at the European level, imply data-base access be granted to a number of authorities with border control attributes (i.e. competent authorities in VISA management and border authorities). In doing so, it raises the question of extending the initial purpose of setting up the system and of the serious impact the subsequent extension of database usage for other purposes it may have on persons.

The fact that the authorized control system at European Union border permits the "human factor" exclusion from the control process, even though it apparently simplifies the passport control procedure, it implies risks concerning personal data processing and keeping to all data subjects' rights.

The National Supervisory Authority has underlined that the introduction of such border control systems imply, for the third country nationals, major risks concerning the respect and guarantee of their rights, since at this stage, through the Schengen borders Code, for example, there are already in effect in depth controls of all third country nationals, both at the entry and at the exist point.

At the same time, even though the main goal of the introduction of an automatic control system at European Union border is that of improving its external borders management, this is one of the means to fight against illegal immigration.

This system is meant to analyze the entry and exist of third parties, which means obtaining a clear image of migratory flows through the external borders.

In this context, it is underlined that "the data processing systems are in the service of the individual; (...) they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy[1] (...)".

Therefore, in accordance with the European Court for Human Rights jurisprudence resulting in breaching Article 8 of the Convention for the protection of human rights and fundamental freedoms, the protection provided by this article would be unacceptably diminished, if the use of modern scientific techniques would be permitted at any cost and without keeping a balance between the advantages of the extensive usage of such techniques and the important interests of private life, and any state that claims a pioneering role in developing new technologies carries the responsibility of obtaining a fair equilibrium in this matter.

Therefore, the National Supervisory Authority has appreciated that, when new large scale

[1] According to recital (2) of Directive 95/46/EC, transposed in Romania by Law no. 677/2001

information systems are proposed and developed, the principle of necessity, proportionality, "taking into consideration of private life starting with the moment when the system is designed" (the so-called "privacy by design" principle) and the principle of purpose limitation have to be observed.

When assessing the provisions proposed by the "Smart Borders" legislative package, the National Supervisory Authority has determined that mainly sensitive data will be processed, among which biometric data, a reason for which it has pointed out that in order to use these data, stringent protection measures should be in place in order to establish the minimum conditions for biometric data usage and to implement backup procedures for persons that cannot be registered.

This legislative package is in the debate stage at European Union Council level.

Section 3: Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a Proposal for a Regulation of the European Parliament and Council on information accompanying transfers of funds

In February 2013, the European Commission has adopted two proposals for consolidating the existing European Union norms regarding the fight against money laundering and transfer of funds. The threats associated to money laundering and terrorist financing are continually evolving, and this issue requires periodical updates of the norms in this matter.

The legislative package includes **a proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as well as a proposal for a Regulation on information accompanying transfers of funds,** for the ensuring of an "adequate traceability" of these transfers.

The common goal of adopting these two legislative instruments is the revision of European Union's present normative system regarding the fight against money laundering and terrorism financing, aiming to raise its efficiency and to ensure its conformity with international standards.

At the European Union level, Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing is instituting the frame meant to protect the solidity, integrity and stability of credit and financial institutions, and the trust in the financial system as a whole against risks of money laundering and terrorism financing.

As for the proposal for a new Regulation of the European Parliament and of the Council on information accompanying transfers of funds, the aim of this act is to revise Regulation (EC) No. 1781/2006 on information accompanying transfers of funds, so that traceability of funds is improved and

the full conformity of the European Union's system with the international standards is guaranteed.

The Regulation on transfers of funds establishes norms, according to which the payment services providers have to transfer information on the payer throughout the payment chain for the purpose of prevention, investigation and prosecution of money laundering and terrorism financing.

The **primary objective** of the legal frame concerning the prevention and fight against money laundering and terrorism financing is to protect the financial system and the free market against abuses on the part of the criminals, who try to launder illegally obtained products , and against terrorists who wish to finance terrorist activities or groups.

As for the **proposal for a Directive of the European Parliament and the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing**, the main proposed changes target:

- he extension of applicability domain of the directive (lowering of level for high value products dealers who execute payments in cash from 15,000 EUR to 7,500 EUR and inclusion in the applicability domain of the directive of "gambling services providers");
- he based on risk approach (completion of the minimum list of factors that have to be taken into consideration or with directions that will be elaborated by the European supervisory authorities);
- simplified and enhanced caution measures concerning the clientage (tightening the norms of simplified caution and eliminating certain exemption situations);
- information on the real beneficiary (new measures are proposed to make information on the real beneficiary clearer and more accessible; by doing this, the legal persons are obliged to hold information on their own real beneficiaries);
- equivalence of third countries (the revised directive will eliminate the dispositions on positive "equivalence", since the caution regime on clientage is more and more based on risk, and the use of exemptions on purely geographical grounds is less relevant);
- administrative sanctions alignment;
- financial information units;
- European supervisory authorities;
- means of transposition (introduction of an obligation for member states to transfer a correspondence table between their national legislative dispositions and the directive's

dispositions).

The introduction of legal provisions on personal data processing in the proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing is justified by the goal of the legislative act itself, which will result in the collection and processing of a very large amount of information, respectively personal data.

This will have direct implications upon natural persons' fundamental rights and may lead, in case of infringement of the law, to severe harms to their privacy, as regards their personal data protection.

Following the analysis of this proposal for a Directive,, in order to ensure a higher legal power to personal data protection and the rights of individuals, the National Supervisory Authority has pointed out that it should exist explicit references to Directive 95/46/EC and to the legislation of the member state concerned on personal data protection also in the content of the articles that refer to data protection.

The proposal for a Directive mentions a period of 5 years as retention period for documents and information, but does not contain also a list of personal data and categories of personal data that are collected from the data subjects and, subsequently, communicated to the competent authorities. This shortcoming leads to uncertainty concerning data processing, but also to certain possible uncertainties in the implementation process of the Directive by the member states.

Related to this aspect, the National Supervisory Authority has appreciated that it would require, in order to eliminate ambiguity, to practically decide upon data and categories of data to be collected and processed, the mere reference to Directive 95/46/EC being insufficient to ensure an adequate level of personal data protection.

Furthermore, the National Supervisory Authority has recommended the insertion of some provisions on confidentiality clauses that have to be kept by the employees of the entities involved in the information reporting procedures, considering the sensitive nature of data to be processed.

Concerning the data protection policies and the policies and procedures on information exchange, the adding of certain mentions referring to the content of these policies, respectively to the fact they have to decide upon adequate technical and organizationally measures for personal data protection against accidental or illegal damages, loses, modifications, disclosure or unauthorized access, as well as against any other form of illegal processing, also considering the disposition of Article 17 paragraph (1) of Directive 95/46/EC was considered to be adequate.

The Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds revised Regulation (EC) No. 1781/2006 on information accompanying transfers of funds to the end of improving payment traceability and ensuring conformity

of EU legislative framework with international standards.

The modifications proposed by the National Supervisory Authority are aiming to identify solutions in the field where problems of transparency still persist, the following main requirements being targeted:

- inclusion of some information concerning the payment beneficiary;

- extension of the applicability domain (including credit and debit cards, mobile phones and any other digital or information device within the object of the regulation's dispositions in case these are used to transfer funds from a person to another and to clarify the funds transfer situation outside of the European Union whose value is less than 1,000 EUR);

- inclusion of new obligations for payment services providers towards the payment beneficiaries (the beneficiary's identity verification in case of payment from outside of EU whose value is over 1,000 EUR), as well as for the payment services provider of the payment's beneficiary and the intermediary payment services provider (the institution of some provisions based on the assessment of risks that would allow the identification of situations in which a transfer for which the required information has not been given has to be executed, denied or suspended and the obligation to decide upon the measures that have to be taken in this respect);

- strengthening the powers to impose sanctions by the competent authorities and the enforcement of the requirement to coordinate actions undertaken in cross-border cases, the publication of the given sanctions and the establishment of some efficient mechanisms in order to encourage the reporting of the infringements of the law cases .

This legislative package is in the debate phase at European Union Council level.

CHAPTER III
REGULATORY ACTIVITY, ADVISING, CONSULTATION AND PUBLIC INFORMATION

Section 1 The approval of legislative acts

By virtue of Article 21 paragraph (3) letter h) of the Law No. 677/2001, the National Supervisory Authority has issued a series of opinions on 32 legislative proposals elaborated by various institutions and public authorities, which referred to aspects concerning personal data processing.

The National Supervisory Authority has formulated relevant observations concerning the legislative acts sent for approval on natural person's rights and liberties protection under the aspect of personal data processing.

Concerning the content of the projects of legislative acts sent to the National Supervisory Authority during 2013, a series of negative opinions, favourable approvals without comments, as well as favourable approvals with comments and proposals have been issued, as follows:

1. ***Negative opinions***

The justificatory arguments for the National Supervisory Authority to issue negative opinions consisted in the lack of correlations of the proposed dispositions with the constitutional principles and regulations, with the European Union's legal acts, with the treaties Romania is a part of or with the specific legislative framework, as well as in generation of parallelisms inside regulations.

Because of this, the National Supervisory Authority has proposed the re-analyzing and the restatement of those proposals for legislative acts.

Among the relevant regulations for which the Supervisory Authority has issued negative opinions we state:

a) Legislative proposal for the collection and retention of necessary data for the identification of electronic communications services' clients delivered through the means of pre-paid cards

The National Supervisory Authority has issued a negative opinion for this proposal, noticing that the initiator didn't take into consideration the fact that he was breaching exactly the European Unions' legislative acts' provisions which the initiator wished to implement. Another infringement noticed by the National Supervisory Authority is the one concerning the observance of privacy, a right consecrated by

Article 26 of the Constitution.

Regarding the processing of the personal identification number of a data subject, which is realized based on conditions provided by Article 8 of Law no. 677/2001, in conjunction with Decision no.132/2011, it has been noted that the proposal seriously violates the principles of proportionality and limited data storage.

By establishing the obligation to communicate the identification data to subjects who have already purchased a service from any type of electronic communications service providers prior to the entry into force of the proposed law, it was considered that it may be contrary to the principle of non-retroactivity of the law, held by Article 15 paragraph (2) of the Constitution.

The imposition on users of electronic communications services provided via prepaid cards, as data subjects, according to Law no. 677/2001, of the obligation to identify or communicate personal data to providers of these types of service (name, surname, personal identification number), is a restriction of their rights, given that exercise trade acts/deeds is conditioned by the proof of identity of the data subjects, and the provision of communications services is subject to certain terms of personal data.

b) The legislative proposal on the social economy (Bp. 439/2013)

The National Supervisory Authority gave a negative opinion on this proposal. The activities carried out in the context of social economy regulation involve performing processing of different categories of personal data, especially sensitive data, such as personal identification number, health, ethnicity, committing criminal acts. This has direct implications on the fundamental rights of individuals and can lead to serious violations of the privacy of citizens in the protection of their personal data.

National Supervisory Authority considered it necessary to define the role and responsibilities of all entities involved in the regulation of social economy and which will process personal data, as well as to establish the powers of public authorities in the collection and processing of personal data in order to clarify their quality as data controllers or data processors, according to the definitions given by Law no. 677/2001.

It has been stressed that it is necessary to take into account the principles of data protection, in particular by establishing authorized persons, as is the case of public authorities and institutions that will have access to data for legitimate purposes and in compliance with all appropriate safeguards for the rights of data subjects.

The activities related to establishing and maintaining of the electronic register of social enterprises and certain reporting requirements (such as those set out in Chapter V of the proposal)

involve collecting and processing of different categories of personal data, including the personal data with an identification function (personal identification number) and other sensitive data.

Concerning the information regarding the state of health, the National Supervisory Authority stressed that it is not only subject to the general provisions of Law no. 677/2001, especially the special provisions of this legislative act. In this sense, Article 7 and Article 9 of Law no. 677/2001 determine, among other things, that the processing of data concerning the state of health is carried out by or under the supervision of medical personnel, subject to professional secrecy or by or under the supervision of another person subject to an equivalent obligation of secrecy.

As for electronic communication data between various entities with responsibilities relating to the electronic register of social enterprises it has been emphasized that such communication may be exposed to a number of risks such as loss, destruction, etc., even accidental of data. However, the choice of methods of transmitting data or documents containing personal data must take into account the fact that data controllers are required to implement appropriate technical and organizational measures to protect personal data. The National Supervisory Authority considered that the implementation of such a system for collecting and processing may represent a new risk for the protection of personal data of individuals and therefore respect and guarantee their fundamental rights, especially the privacy, because it relies on the collection and processing of various types of personal data, especially those of a sensitive nature.

Because it concerns the processing of sensitive data that require adequate protection, and the text of the legislative proposal on the social economy does not detail enough concrete data processing methods and the method of exercising the rights of data subjects, in particular the right of access, it has been requested its reconsideration.

c) The legislative proposal amending Law no. 544/2001 on free access to public information (Bp. 584/2013)

The National Supervisory Authority has given a negative opinion since the provisions of the legislative proposal amending Law no. 544/2001 refer to a variety of personal data of employees of a public institution or authority which would be disclosed to the public through their websites. Thus, it was proposed the disclosure of the name, education background, professional experience, IT skills, language skills, wages or otherwise, or of other personal data included in the curriculum vitae of personnel or detached from an authority or public institution.

These data not only directly and specifically identify a person, but also publicly expose, to a

large extent, the privacy of the data subject by reference to the multitude of "specific factors to his physical, physiological, mental, economic, cultural or social identity".

Law no. 677/2001 establishes the conditions under which personal data may be processed, and even disclosed to third parties. Personal data may be processed by a data controller (public institutions and authorities, in case of the Law no. 544/2001), without the consent of the data subject, in exceptional circumstances, the strict interpretation and application, governed by Article 5 paragraph (2) of Law no. 677/2001. The processing of personal data and the disclosure of personal data to the public, contained in the legislative proposal, by posting on the Internet indefinitely, are operations that may lead to increased risks to the rights and freedoms of data subjects publicly being exposed by excessive processing of their data, based on the intended purpose.

Excessive exposure of personal data of persons occupying certain positions within a public authority or institution is not only likely to affect private life, honour and dignity, and possibly that person, but also exceeds the principle of "transparency" and "need to know" invoked by the initiator of the legislative proposal.

As to the public interest, which in the initiator's view "is above private", we emphasize that such compliance cannot be invoked at any cost, at the expense of privacy, without considering justified situations.

When the fundamental right to privacy, especially the protection of personal data, faces other fundamental rights, such as the right to information, it must found a balance in their compliance.

d) The legislative proposal amending and completing certain provisions concerning civil status and processing of personal data

In regard to the future amendment of Law no. 677/2001, the National Supervisory Authority has formulated a negative opinion and stated that the current provisions of the law allow the processing of personal data in order to ensure proper implementation of the new Civil Procedure Code.

Regarding the proposed amendment by the legislative proposal submitted for the purposes of completing Article 5 paragraph (2) of Law no. 677/2001 by introducing new exceptions from the consent of the data subject, it has been stated that it is not required that filling enactment as personal data can be revealed if there is a legal obligation of the data controller or when the data is required in pursuit of a legitimate interest of the data controller or of the third party to whom such data is disclosed, according to Article 5 paragraph (2) letter c) and e) of Law no. 677/2001.

Regarding the introduction of the proposal submitted to a new situation in which processing the

personal data with an identification function (e.g. personal number, serial and no. of identity document) is allowed, by the completion of Article 8 of Law no. 677/2001, the National Supervisory Authority has stated that it is not necessary to complete such enactment, as this category of personal data can be revealed when there is an express legal provision according to the current provisions of Article 8 letter b) of Law no. 677/2001. In addition, it was noted that it is not mandatory to mention the personal identification number of the parties on the application for summons as Article 194 of the Civil Procedure Code provides that it is indicated to the extent it is known by the applicant.

On the proposed amendment by the legislative proposal submitted for the purposes of introducing a new Article 8^1 within Law no. 677/2001, which was intended to establish the obligation to hand out immediately a document containing the personal data requested by a third party for the establishment, exercise or defence of legal claims, it was considered that this provision is not likely to provide a review corresponding to that request by the public authorities responsible so as to prevent unlawful disclosure of personal data that can seriously affect one's life.

On the other hand, regarding the proposed amendment of Law no. 119/1996 on civil status, republished, with subsequent amendments, it was considered not necessary to amend or supplement this legislation.

Thus, the issuing of extracts of civil status is governed by the relevant provisions of Article 69 and Article 70 of Law no. 119/1996 that determine the categories of authorities (including courts of law) and entitled people to communicate extracts from civil status of individuals, under their legal powers.

Unjustifiably expanding the sphere of persons to whom it can be issued extracts from civil status of other persons (which contain a lot of personal data) can seriously undermine the right to protection of personal data and privacy of individuals.

e) The draft for Norms for applying Law no. 82/2012 on the retention of data generated or processed by providers of public electronic communications networks and publicly available electronic communication services providers and amending and supplementing Law no. 506/2004 on the processing of personal data and privacy in the electronic communications sector

In regard to the submitted document, the National Supervisory Authority has formulated a negative opinion, underlying that the draft of Law no. 82/2012 also received a negative opinion from the Supervisory Authority, as it contains mostly identical provisions with the ones of Law no. 298/2008, a law declared unconstitutional by the Constitutional Court Decision no. 1258 of 8 October 2009.

2. Favourable opinions, without comments

In 2013, the National Supervisory Authority issued favourable opinions without comments, to the drafts of legislative acts that were in compliance with the provisions in the field of personal data protection, among which we mention:

- Draft law on amending and supplementing Law no. 334/2006 on the financing of political parties and election campaigns;

- The draft of Government Ordinance to create the necessary legal framework for automated searching of reference data in relation to the European Union Member States and ensuring recognition results of laboratory on fingerprint data;

- The draft law regarding the approval of Government Emergency Ordinance amending and supplementing certain legislative acts on tracking persons, identity documents of Romanian citizens and residence documents of citizens of Member States of the European Union and European Economic Area residents in Romania;

- Legislative proposal regarding the amendment of the Law on political parties no. 14/2003;

- The draft law regarding the approval of Government Emergency Ordinance amending and supplementing certain acts on tracking persons, identity documents of Romanian citizens and residence documents of citizens of Member States of the European Union and European Economic Area residents in Romania;

- The draft law on some measures to facilitate cross-border exchange of information on traffic violations affecting road safety.

3. Favourable opinions with comments and suggestions

As for favourable opinions issued in 2013, the National Supervisory Authority has made numerous observations and proposals aimed at providing a complete regulation and a clear drafting of legislative acts, in order to understand and apply them correctly.

In this context, we mention that most of the comments and proposals made by the Supervisory Authority have been acquired by the initiators. Of the draft legislation on which the Authority has formulated proposals, we mention:

a) Draft Law amending and supplementing Government Emergency Ordinance

no. 195/2002 on public road traffic

The National Supervisory Authority stressed out that the draft contained provisions requiring clarification and recommended reconsideration of the legal text proposed for approval. Regarding the term for storing of personal data consisting of image and voice, referred to by the project, it was highlighted that it must be consistent with the provisions of Article 4 paragraph (1) letter e) of Law no. 677/2001, specific measures taken and developed by Decision no. 52/2012 concerning the processing of personal data through the use of video surveillance, issued by the National Supervisory Authority.

At the same time, following the analysis of the project, it was pointed out that personal data may be exposed to a number of risks such as loss, unauthorized disclosure or access, issues that could have a significant impact on the privacy of citizens in the protection of their personal data, with reference to their disclosure by transmission or by publication, reason for which the provisions of Article 20 of Law no. 677/2001 must be kept.

In addition, it was shown that data controllers have specific obligations incumbent upon the rights of data subjects—in particular, the right to information, access to data and intervention upon data, according to Law no. 677/2001.

b) The draft Emergency Ordinance amending and supplementing Law no. 95/2006 on healthcare reform and amendment of some acts

The National Supervisory Authority has approved the project, but made the following observations:

In the context of electronic communications data by medical services providers to various entities (Ministry of Health, the structures of the Ministry of Health, the National Health Insurance, etc.) with specific tasks, it must be kept in mind that when choosing the methods for transmitting data or documents containing personal data, such services, as data controllers, have an obligation to apply appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, in particular where such processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The National Supervisory Authority mentioned that the institution that is responsible for the organization and administration of health insurance information platform is the National Health Insurance Fund, as data controller, and it is required to ensure confidentiality and security of data processing performed in the context of the need for platform interoperability of e-Health solutions at national level.

The above mentioned obligationalso falls upon the Ministry of Health, in the context of exchanging information with other EU member states that cooperate within a voluntary network connecting national authorities responsible for e-Health designated by Member States.

c) The legislative proposal introducing courses in Romanian language, literature and history via internet for Romanian citizens' children living abroad

In order to establish the point of view of the Government, the National Supervisory Authority has formulated comments and suggestions.

Thus, it was found that implementing an electronic system for the collection and processing of minors' data on the Internet, through online forms, is likely to present specific risks to the rights and freedoms of this category of persons. Therefore, providing an effective protection of personal data, in accordance with the provisions of Law no. 677/2001, is very important, but there must be also considered the legal provisions which guarantee the rights of children.

Consequently, for respecting the fundamental rights of minors, in particular the right to privacy, the National Supervisory Authority has appreciated the need for the insertion of provisions in the legislative proposal relating to the processing of personal data in compliance with Law no. 677/2001.

d) Legislative proposal to Government Ordinance no. 2/2001 on the legal regime of contraventions

The National Supervisory Authority has approved a legislative proposal, with the following mentions:

Regarding the conclusion of the minutes of offence also in electronic form, it was considered that the implementation of such system for collecting and processing data through automated systems can be exposed to a number of risks such as loss, destruction, etc., even accidentally.

It was noted that by this legislative proposal, there are introduced new ways of communicating offence minutes, but also notification of payment, without specifying the exact applicable procedure and without taking into account the applicable legal provisions, including the provisions of Article 5 paragraph (3) of Law no. 677/2001, which obliges public authorities to respect and protect the privacy, even in the case of exemption from the rule obtaining the consent of the data subjects.

e) The legislative proposal amending and supplementing Law no. 334/2006 on the financing of political parties and election campaigns

Although the National Supervisory Authority has approved the legislative proposal it has made also comments in light of the fact that the proposal has direct implications for the fundamental rights of individuals and may lead to serious privacy violations of citizens in terms of data protection of their personal data, especially in the case of disclosure of such data publication on the website of the data controller (Permanent Electoral Authority).

The National Supervisory Authority highlighted that it is necessary to follow the principles established by Article 4 paragraph (1) of Law no. 677/2001, and especially the principle that data should be stored in a form which permits identification of data subjects for the duration strictly necessary to achieve the purpose of processing, which involves setting limits on disclosure of personal data on the Internet, given risk posed by disclosure of the data in the context of online privacy enforcement.

Also, the National Supervisory Authority has mentioned the need to take into account also the fact that data controllers are required to implement appropriate technical and organizational measures in order to protect personal data.

f) Draft Law on amending and supplementing Law no. 7/2004 on the Civil Servants Code of Conduct

Related to this project, the National Supervisory Authority has recommended the introduction of a provision relating to the fact that the processing of personal data shall be carried out in compliance with Law no. 677/2001, including the exercise of the rights of data subjects, of the measures of security and confidentiality of the processing performed.

g) Draft Government Decision regarding the approval of the Methodological Norms for implementation of the provisions of the Convention no. 16 of the International Commission on Civil Status issue of multilingual extracts from civil status acts, signed at Vienna on September 8, 1976

Regarding the issuing of multilingual extracts, the National Supervisory Authority highlighted that in the draft text there should be considered the need to respect the obligation of the data controller to take appropriate technical and organizational measures to protect personal data in accordance with Article 20 of Law no. 677/2001.

In this regard, in order to strengthen compliance with the law, it was considered necessary to insert some mentions regarding the security of the data in their transfer activity between institutions, which have in custody civil status documents and which receive requests of issuing statements,

respectively issue statements, since the communication can expose personal data to a number of risks such as loss, destruction, etc., even accidentally.

The National Supervisory Authority considered appropriate to add a provision, in the content of which to be stated the fact that transmitting multilingual extracts will be subject to the measures of confidentiality and security of personal data, especially considering that in some cases is carried out, in reality, a transfer of data outside the European Union.

h) Draft Government Decision approving the Framework Agreement on the conditions of medical assistance in the health insurance system for the years 2013-2014

The draft contains, in many cases, the obligation of data controllers from the field, the health insurance funds and health care providers, to communicate personal data frequently, especially sensitive data (such as your CNP, data on the state of health, diagnoses, medication, etc.), both by physical media and by electronic means of communication.

The National Supervisory Authority has approved the project, but highlighted that the data can be exposed to a number of risks such as loss, unauthorized disclosure or access, issues that could have a significant impact on the privacy of citizens.

Direct online access to databases presents a new risk, both by the fact that personal data will be disclosed to a large number of recipients, and bythe fact that it will provide new opportunities for their possible misuse. Thus, these systems must ensure that only authorized individuals have access to data, for legitimate purposes and in compliance with all legal guarantees. At the same time, multiple access points in an open network, such as the Internet, increase the risk of interception of personal data, and once they are available to a large number of people, it will become difficult to maintain an adequate confidentiality standard for protecting the data.

Related to the above issues, it was considered that it is necessary to complement the text of the draft framework-contract by strengthening the liability of data controllers relating to the data processing. In order to comply with the whole system of protection of personal data, not just the one referring to confidentiality, it is required to comply with all the rules on personal data protection, much more because some of the data collected are of a sensitive nature (state of health).

Regarding generic formulations of the draft, respectively "copies of documents", "justifying documents", "accompanying documents", according to the principle of purpose proportionality, stated in Article 4 paragraph (1) letter c) of Law no. 677/2001, it was highlighted that the data must be adequate, relevant and not excessive in relation to the purpose for which they are collected and further

processed. In this respect, it was underlined to consider the express mention (in methodological norms), of the necessary documents, which contain also personal data, required from individuals, in order to prevent in practice an inconsistent and abusive conduct, under these circumstances.

The same principle mentioned above must be respected also in terms of developing a standard questionnaire for conducting surveys to monitor the satisfaction of policyholders. The National Supervisory Authority considered it necessary to mention, in methodological norms, that the data should be stored, for a certain period of time, in a filing system different from the one that refers to the effective provision of health services, as well as the rendering of the data anonymous or even its collection, to the possible extent, should be made anonymously, without carrying out a connection with the insured.

i) Memorandum entitled "Approval for initiation of negotiations and signing of the Agreement between the Government of Romania and the Government of the United States to improve international tax compliance and implementation of FATCA"

The National Supervisory Authority has made some comments on the need to incorporate explicit claims regarding compliance with the adequate protection of personal data provided in the Member States of the European Union and therefore in Romania by Law no. 677/2001.

Given the nature of the data collected and processed, it was highlighted the need to clarify the text of the agreement, particularly with regard to the data retention period, ensuring the confidentiality and security of personal data, the rights of the data subject and how to exercise them.

j) Draft resolution of the Permanent Electoral Authority regarding the drafting and the approval of the lists comprising persons who may be appointed presidents of the polling station or their deputies

It was noted that in the project it is created a situation of discrimination against other categories of persons, based on the nature of the data collected and processed, as well as on the evaluation of these people based on the information collected, an aspect that should be corrected.

The National Supervisory Authority considered necessary to establish some claims regarding the period of information storage and obligation to delete/destroy personal data by each entity that processes data.

Regarding the method of processing the personal identification number and the copy of the identity card, it was pointed out that it must comply with the provisions of Article 8 of Law no. 677/2001.

Section 2. Views on various issues on data protection

A. Applicability of Law no. 677/2001

1. The National Commission for Accreditation of Hospitals has asked the National Supervisory Authority's view on the need to notify the data processing they perform in the preparation, qualification and training of hospital assessors.

In regard to related issues concerning the functions of the National Commission on Accreditation of Hospitals, by reference to the provisions of Law no. 677/2001, this institution was informed that is required to declare to the National Supervisory Authority the processing of personal data carried out in the preparation, qualification and training of assessors hospitals, sense in which were given details relating to notification procedure.

At the same time, the institution was informed that, distinctively, will notify the National Supervisory Authority about the data processing carried out by video surveillance means, in accordance with Article 15 of the Decision no. 52/2012.

Moreover, the National Commission for Accreditation of Hospitals was made aware of the obligations to which it is held as data controller mainly that of compliance with the legal provisions concerning the exercise of the legal rights by the data subjects, respectively the right to information, access, intervention and opposition, as well as the obligation to ensure confidentiality and security of processing carried out, in accordance with the provisions of Law no. 677/2001.

Regarding the matter of the publication on the website of the institution of statements from the hospitals register assessors, that contain the name and surname of the assessors, profession, series and date of the authorization as evaluator, our institution has drawn attention to the fact that personal data may be disclosed to third parties only in cases where the data subject has given express and unequivocal consent or in exceptional conditions established by Article 5 paragraph (2) of Law no.677/2001.

2. An individual addressed the National Supervisory Authority requesting opinions on his quality of data controller, if he intends to process personal data by video surveillance means, mounted on home balconies, but directed on access doors in a building with several apartments.

It has been stated that, within the meaning of Article 3 letter e) of Law no. 677/2001, the data controller is also a natural person who determines the purpose and the means of processing personal data. At the same time, in accordance with Article 2 paragraph (6) of Law no. 677/2001, this legislative

act does not apply to the processing of personal data, carried out by natural persons exclusively for their personal use, if the data in question is not intended to be disclosed.

These provisions are reiterated also by Article 17 paragraph (2) of the National Supervisory Authority Decision no. 52/2012 concerning the processing of personal data through the use of video surveillance.

As such, it was considered that, in so far as it complies with the condition established by Article 2 paragraph (6) of Law no. 677/2001, the individual does not have a data controller status and, therefore, any of his obligations.

But, where that data will be revealed to various recipients (except public authorities which may receive data in a particular inquiry), that individual will acquire the status of a data controller, with the obligations imposed by the legislation in the field, including the one regarding the notification.

The National Supervisory Authority also stated that the video surveillance may be carried out in open places and spaces or intended for the public, including public access ways on private or public property, as provided by law, with the condition that the cameras should be in conspicuous places.

In this context, the National Supervisory Authority also specified that data controllers performing video surveillance, in order to monitor access or to ensure the safety of property and/or persons, are obliged to inform adequately or in a clear and permanent manner about the existence of video surveillance system (poster, ad) and, also, to ensure the database security. At the same time, there was also provided information on the storage period allowed and the measures to be taken at the deadline.

3. An individual has requested the National Supervisory Authority's point of view regarding the applicability of Law no. 677/2001 in the activities of a pawnshop.

From those shown in the address, based on Law no. 677/2001, references were made to the effect that:

- the company is required to analyze (in relation to all activities) whether it carries out data processing; to the extent to which personal data is processed, being set out the purpose and the means of data processing, the company has the quality of data controller and the incumbent obligations established by Law no. 677/2001.

- it has been highlighted that it is necessary to notify the processing performed by the data controller that processes personal data, in so far as the provisions of Decision No. 90/2006, Decision no. 100/2007 and Decision no. 23/2012, issued by the National Supervisory Authority, referring to

situations where it is not necessary to notify the processing of personal data are not applicable;

- based on the work of a "pawn shop", the company to which reference is made, has the quality of data controller and must notify the Supervisory Authority about the data processing of clients (individuals) to "other lending activities—pawn";

- there were presented the necessary stages in order to obtain the registration in the electronic register of processing personal data.

4. The Bucharest Autonomous Public Transport requested the point of view on the exemption from notification of processing operations performed in the current work, considering the fact that operates under the authority of the General Council of Bucharest.

The National Supervisory Authority specified that the situations are not applicable for exemption from the notification requirements of Decision no. 23/2012 on the establishment of the cases where it is not necessary to notify the processing of personal data, issued by the Supervisory Authority.

At the same time, it was highlighted that, related to the purposes in which the Autonomous Public Transport processes personal data, there are applicable the exemptions from the notification requirement of Article 1 letter a) - f) of the Decision no. 100/2007 regarding the establishment of the cases in which it is not necessary to notify the processing of personal data, issued by the National Supervisory Authority.

It was also noted that, in cases where exceptions are applicable from the obligation to notify the processing performed, the data controller is not relieved from meeting other obligations imposed under the laws applicable to the protection of personal data (informing data subjects, exercising the data subjects' rights, confidentiality and security of processing).

5. The Ministry of Labour, Family and Social Protection requested the National Supervisory Authority’s point of view regarding the processing of personal data carried out for the purpose of a survey among its employees, through a company which owns an online data collection platform.

From the forwarded address it appeared that this ministry is the one that established the purpose of data processing of its own employees (for making a survey), and the survey would be conducted by a company, with which a service contract will be concluded, and which, according to Law no. 677/2001, has the quality of data processor, while the processing shall be performed by means of a technical platform for on-line data collection.

Related to these issues, the National Supervisory Authority has stated that:

- the data processor is a natural or legal person, private or public law, including public authorities, institutions and their territorial entities that process personal data on behalf of the controller;

- the obligations to notify the National Supervisory Authority of the processing fall on the data controllers, and not on their data processors;

- carrying out processing by data processor must be conducted under a written contract, which shall include the mandatory obligation of the data processor to act only on instructions received from the data controller and that the obligations on the implementation of security measures returns on data processor;

- in order to obtain registration in the electronic register of personal data processing it must be filled out the notification form, which contains also a section on data transfers, respecting the notification procedure (submission of on-line notification and transmitting the first page from this form, completed and signed, in original).

6. In another situation, information was requested regarding the applicable law for the processing of personal data of minors, in the context of achieving an IT application for children.

Regarding the operations of collecting personal data of minors via the Internet, it was stated that they are likely to present specific risks to their rights and freedoms, so that the data controller needs to consider ensuring effective protection of minors.

It was also mentioned that the legal provisions, which guarantee the rights of children to protect their public image, personal, private and family life, protection against all forms of exploitation, abuse, etc., must be taken into consideration.

Thus, it was found that, depending on the age of the minor, the legal representative can be asked for some contact information (telephone number, e-mail etc.) in order to contact them or can make the use of various computer applications or enrolment sites only by parents. In all cases, the manner from which results that the legal representatives of minors give their express and unequivocal consent is to be chosen so as to be able to be proved, if so required and there must exist the certainty of its origin.

In addition, when using electronic means of communications, it was stated that it is necessary to consider the provisions of Article 12 of Law no. 506/2004 on the processing of personal data and privacy in the electronic communications sector, as amended and completed, in order to obtain prior express consent of the recipient for sending commercial communications by such means.

7. An individual has requested information regarding the processing of personal data for literary

and artistic purposes.

Clarifications were made on the applicability of Article 11 of Law no. 677/2001, where data is processed exclusively for journalistic, literary or artistic purposes, these being achieved without the consent of the data subjects, with the condition that such data has been manifestly made public by the data subject or has been closely related to the quality of a public person of the data subject or the public nature of the facts involved.

If the statutory conditions above mentioned are not met, it is necessary to obtain the consent of the data subjects (or their heirs, in the case they are deceased).

Among other cases of exception from the obligation to obtain the consent of the data subject are also those governed by Article 5 paragraph (2) of Law no. 677/2001, as further amended and supplemented, namely the legitimate interests of the controller or the third party to whom the data is revealed. But in this situation, it is also necessary to respect the rights and freedoms or the interest of the data subject, but also to inform and obtain the consent of the data subject for the disclosure of their data in the artistic documentary, if the situation does not fall under Article 11 of Law no. 677/2001, as further amended and completed, mentioned above. With regard to the legitimate interest, it must be fully justified and evidenced by certain documents.

In conjunction with the above, Law no. 677/2001 establishes the principle of purpose proportionality, in Article 4 paragraph (1) letter c). This principle must be respected, regardless of the legitimacy conditions of processing, namely on the basis of consent of the data subject or on the basis of the exception to consent.

Accordingly, personal data may be disclosed without the consent of the data subject, only in the exceptional legal conditions set out above, respecting the principle of purpose proportionality. In this respect, the purpose of the requested data (or their disclosure) should be placed in a situation of exception to consent.

It was also stated that the provisions of Article 10 of Law no. 677/2001 refer to the processing of personal data relating to criminal offences or misdemeanours.

On this occasion, it was stated that, according to Article 1 letter k) of Decision no. 100/2007, the notification of personal data processing is not required when personal data processing is carried out solely for journalistic, literary or artistic purposes. Therefore, for data processing performed within literary activities it is not necessary to register a notification in the electronic register of the processing of personal data.

8. An individual has submitted a request to the National Supervisory Authority under Law

no.544/2001, with amendments and additions. . Towards its content, there were made few observations:

Thus, on the first request, it was highlighted that the name, forename, position, workplace, in the sense of Article 3 paragraph (1) of the Law no. 677/2001, as amended and completed, are personal data.

As for the second request, on the data controller quality, in the context of posting articles on the site, it was stated that the person (natural or legal person as appropriate) who wrote the article and the domain holder, as well, can act as data controllers, when performing processing operations on personal data, determining the purposes and means of processing such data.

Regarding the third request about the obligations of the data controller, it was mentioned that any data controller (natural or legal) is held responsible to respect all the data subject rights, under Law no. 677/2001 as right to information, right to access to data, right of intervention upon data and the right to object.

As to the fourth request, about the obligations of a domain holder in the context of posting of articles, it was specified that in the event that the holder acts as a data controller, establishing the data processing means, it is held by respecting all rights of the data subject.

At the same time, if the domain owner only posts the data and does not perform any data processing operation on them, it has the quality of a third party, in the sense of Article (3) letter g) of Law no. 677/2001.

In these circumstances the provisions of Article 5 of Law no. 677/2001 are applicable, under which personal data may be processed or disclosed to third parties only if the data subject has given express and unequivocal consent or, in exceptional cases, without express consent, as provided for in Article 5 paragraph (2) of the Law no. 677/2001.

Regarding the last request, referring to the penalties that can be imposed by the National Supervisory Authority, the provisions of Articles 31-34 of Law no. 677/2001 were pointed to.

9. A petitioner requested the opinion of the National Supervisory Authority on the need to notify the data processing of owners and tenants, carried out by an association of owners, when carrying out activities related to their record.

Related to the issues raised, the National Supervisory Authority said that the owners and tenants' data processing, carried out by the association exclusively for the building management, does not require submission of the notification, according to Article 1 letter c) of the Decision no. 90/2006.

At the same time, the petitioner was informed that, although in the above-mentioned situation the notification shall not be required, the homeowners association, as data controller within the meaning of

Law no. 677/2001, as amended and completed, is bound by compliance with the requirements of Article 12 and Article 20 of Law no. 677/2001, to inform the owners, as data subjects, as well as to respect the security and confidentiality of personal data.

Observations were given about the need to notify data processing, in the situation where the association will perform such operations, through the use of video surveillance means, with the possibilities to record and store images and data.

B. Reporting to the Credit Bureau

It was requested the National Supervisory Authority's point of view regarding the reporting conditions for bank customers towards S.C. Biroul de Credit S.A.

The legal conditions for processing personal data in record systems, such as credit bureaus, were regulated by the National Supervisory Authority by issuing Decision no. 105/2007 on the processing of personal data carried out in record systems of credit bureau type.

Article 8 paragraph (1) of Decision no. 105/2007 lays down the rule to personal data reporting to the record systems of credit bureau type, respectively only with the written consent of the data subject, obtained by the participants at the time of application for credit. In this regard, when obtaining the agreement, it is necessary to achieve and inform the data subject, in order for him/her to give his/her informed consent.

The same Article 8 paragraph (2) provides that the negative data, including those resulted from application of fees or interest rate hikes, are transmitted to systems of credit bureau type only after prior notification, made by the participants in writing, by phone, SMS or via e-mail, of the data subject about late payments and transmission of data, performed at least 15 days before the date of transfer.

The National Supervisory Authority considers that the prior notice of the data subject with at least 15 days before the date of submission to the credit bureau, that contains the information set out inArticle 9 of Decision no. 105/2007, must be made before the first reporting to the credit bureau, as a result of accumulation of arrears, as well as every time when a new arrear is registered, in the context of payment of monthly rates, different from the previous one.

If this right is disregarded, the act may fall under Article 32 of Law no. 677/2001, referring to the sanctioning of unlawful personal data processing by a data controller.

In the reply, references were also made to Article 15 paragraph (1) of Law no. 677/2001, as amended and completed, that the data subject has the right to object at any time, on compelling legitimate grounds relating to his particular situation, the data that are intended to be processed, unless

there are contrary legal provisions.

In order to exercise the right guaranteed by the law mentioned above, the data subject has the opportunity to submit an application to the banking company in question, that shall be in writing, dated and signed, and the latter is required to communicate a response within 15 days of the receipt of application.

If, after the expiry of the 15 days period, which begins on the date of the notification, the data controller has not received an answer or a request has not been resolved, the data subject may appeal to the National Supervisory Authority.

C. The processing of the personal identification number on invoices

The companies continued to require the National Supervisory Authority's point of view on the necessity of processing the personal identification number on invoices and also on the quality of the data controller of such companies.

It was highlighted that a company's financial and accounting activities fall within the provisions of Article 1 letter a) of Decision no. 100/2007, that the notification shall not be required when "the data processing is performed by departments/persons competent of public and private entities, in order to satisfy the requirements of the law for their current organization and performance management—financial and administrative."

It was shown that a data controller that is not required to notify certain data processing has to respect other obligations arising from the provisions of Law no. 677/2001, as amended.

With regard to the processing of personal identification number, it was highlighted that, according to Article 8 of Law no. 677/2001, as amended and completed, this may be done only if the data subject has given express consent or if the processing is provided expressly by a statutory provision.

Correlated with the above mentioned provision, Article 4 paragraph (1) letter c) of Law no. 677/2001 states that personal data intended to be processed must be adequate, relevant and not excessive in relation with the purpose for which they are collected and further processed. These characteristics of personal data involve the data controller's obligation to ensure, in its processing activity, the adequate, relevant and not excessive character of the data.

It was stated that there are no expressed legal provisions in force in the Fiscal Code regarding the collection of personal numeric code in any situation on the preparation of tax invoices for beneficiaries-individuals as buyers of a product or service.

Thus, according to Article 155 paragraph (19) letter d) and f) of Law no. 571/2003 regarding the Fiscal Code, as amended and completed, among the required data necessary to complete the invoice, it should be included the: name, address and the registration code for VAT purposes and, where appropriate, the fiscal identification number of the taxable person, supplier of goods or services, or the name and address of the beneficiary of goods or services, as well as the registration code for VAT or tax identification code of the beneficiary, whether it is taxable or non-taxable legal person.

According to Article 127 paragraph (1) of the Fiscal Code, the taxable person is any person who develops, in an independent manner and regardless of the place, economic activities of the kind referred to in paragraph (2) of this article (e.g. activities of producers traders or providers of services, including mining, agricultural and free professions or assimilated activities, exploitation of tangible or intangible property for the purpose of obtaining incomes on a continuous basis) for any purpose or result of this activity.

Therefore, only if the beneficiaries of the goods purchased are taxable, for the purposes of legal provisions above, since there is a legal basis, the invoice will contain the tax identification code/personal identification number.

D. Disclosure of personal data

1. The Superior Council of Magistracy has requested the National Supervisory Authority's point of view in relation to the disclosure of personal data contained in the declarations provided by Article 5 paragraph (3) of Law no. 303/2004, republished, in the context of Article 14 paragraph (1) of Law no. 544/2001.

In regard to the provisions of Article 5 paragraph (3) of Law no. 303/2004, republished, it was appreciated that there is no legal obligation on disclosure, by the institution holding, of the personal data contained in the documents from the personnel file of judges, prosecutors, assistant-magistrates and support staff, required to give annually a self-responsibility statement whether the husband, relatives and affidavits up to the fourth degree including, exercise a function or perform a legal activity or investigative on criminal activities, as well as their working place.

On the other hand, it was stated that personal data may be disclosed in order to achieve a legitimate interest of the one requesting data, only if such interests are not overridden by the interests or fundamental rights and freedoms of the data subject. In this respect, it is necessary to take steps not to harm the interest or the rights and freedoms of the data subject.

So, where there is a legitimate interest from the part of the data requestor, it was held that the

interest must be fully justified and proven, while respecting the rights of the data subject, in particular the right to information and to object, according to Articles 12 and 15 of Law no. 677/2001.

In other words, the data subject must be informed of the request for disclosure of information concerning it, to give the opportunity, for good reasons related to his particular situation, to object to the disclosure of the data.

In conjunction with the above, Law no. 677/2001 establishes the principle of purpose proportionality, in Article 4 paragraph (1) letter c). According to this, the data processed by a data controller must be adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed (including disclosed). This principle must be respected, regardless of the legitimacy of processing, namely on the basis of consent of the data subject or on the basis of the exception to consent.

Accordingly, personal data may be disclosed, where the data subject's consent does not exist, only on the exceptional legal conditions, provided by Law no. 677/2001, respecting the principle of purpose proportionality. In this respect, the purpose of the request of data (or their disclosure) should be placed in a situation of exception to consent.

2. The National House of Public Pensions (CNPP) has requested an opinion on the application of financial non-banking institution addressed to the CNPP on the conclusion of a "Convention to update/provide basic identifying jobs of its customers."

From the analysis of the mentioned request and the documents attached, it resulted that the financial non-banking institution has requested CNPP the disclosure of personal data, arguing that there is a "legitimate interest".

It was also showed that the information on work place is updated by the client "within 3 days from the date of the change, if any."

In this context, it was stated that Law no. 677/2001, as further amended and supplemented, establishes the conditions under which personal data may be processed, including disclosed. Under this legislation, the general rule governing the processing of personal data is the data subject's consent, given expressly and unequivocally.

Exceptionally, however, personal data may be processed (including disclosed) by a data controller, without the consent of the data subject, in many cases of exception, of strict interpretation and application, regulated by Article 5 paragraph (2) of Law no. 677/2001.

In this context, it was noted that in the National Bank of Romania's Regulation no. 9/2008, on

knowing the clientele, with the purpose of preventing money laundering and terrorist financing, raised by the financial non-banking institution, appears that at the moment of identifying individual customers, it should be considered obtaining of information on a range of data, including the name of the employer.

At the same time, the text of the Regulation does not detach the obligation to obtain, by legal persons subject to the regulation, his employer's information on behalf of the entities they own.

When invoked to achieve a legitimate interest of the applicant requesting the data, it may be legal basis for the request data only if such interests are not overridden by the interests or fundamental rights and freedoms of the data subject. In this respect, it is necessary to take steps not to harm the interest or the rights and freedoms of the data subject.

So, where there is a legitimate interest of the financial non-banking institution (client failing to update his/her data), we consider that it must be fully justified while respecting the data subject's rights, especially the right of information and right to object, according to Articles 12 and 15 of Law no. 677/2001.

In line with the above, the provisions of the Civil Procedure Code in force, in matters of enforcement, establish that if the debtor does not voluntarily execute the obligation established by an enforceable, it shall be brought out by enforcement, starting with notification of the enforcement body, in accordance with Book V of the Code, which is the common law enforcement, regardless of the source or nature of the obligations contained in enforcement or legal quality of the parties (Article 622 in conjunction with Article 631 paragraph (2) of the Civil Procedure Code). In conformity with that Code, enforcement of any enforceable (...) shall be made only by the judicial executor, even if the special law provides otherwise (Article 623). Also, according to Article 625 of the Code, the enforcement is done in compliance with the law, the rights of the parties and other interested persons.

In regard to these provisions and taking into account the principle of the legitimacy of the purpose, the Authority judged that the processing of information regarding the employer’s name, by the financial non-banking institution, can only be achieved with the purpose of updating the data in question, with the condition of respecting the guarantees provided by the Law no.677/2001, mentioned above, and to fulfil, according to the law, the enforcement procedure.

3. The Bucharest Autonomous Public Transport (RATB - urban transport) requested an opinion on the request of a union entity to disclose personal data of employees belonging to urban transport.

The National Supervisory Authority mentioned to RATB that where a trade union entity will invoke the existence of a legitimate interest (e.g. representing the interests of employees, union

members, whose data is required), it will have to prove the existence of the legitimacy of their interest to obtain data from RATB for each individual whose data is required.

Moreover, if the aforementioned evidence will be given, it will be mandatory to respect the rights of persons concerned, respectively informing the data subject right, before disclosure, according to Article 12 paragraph (2) of Law no. 677/2001, and respect the right to object of the persons involved (urban transport employees).

Consequently, the National Supervisory Authority has assessed that the disclosure of personal data by RATB can be made under the provisions of Article 5 paragraph 2 letter a) of Law no.677/2001, but only if the rights of persons involved are respected and to the extent to which the entity union will prove the legitimacy of its interest.

4. The Maramureş Department of Agriculture asked for our point of view on the terms of disclosure for the employees' personal data following the media's request.

The National Supervisory Authority highlighted that the rule established by Law no. 677/2001 is that the processing of personal data of an individual (including disclosure) by another person or entity, as data controller, is carried out with the consent of the data subject, given expressly and unequivocally. Exceptionally, by the provisions of Article 5 paragraph (2) of Law no. 677/2001, there are also expressly established certain exceptions from the requirement to obtain consent to the processing of personal data and, implicitly, their disclosure.

At the same time, we mention that, according to Article 12 letter d) of Law no. 544/2001 on access to public information, as amended and supplemented, information on personal data, according to the law, is exempt from free access of citizens.

Therefore, in the presented situation, disclosure of personal data of employees (including their timesheets) cannot be made without their express and unequivocal consent.

5. An individual has requested information on the legal framework governing the disclosure of data regarding the state of health.

Law no. 677/2001 establishes the principle of purpose proportionality, stated in Article 4 paragraph (1) letter c), that must be respected, regardless of the legitimacy of processing, namely on the basis of the consent of the data subject or on the basis of the exception to consent.

Concerning the data regarding the state of health, we highlight that these are sensitive data protected by special rules introduced by Law no. 677/2001.

Data processing conditions on state of health are set out in Article 7 and Article 9 of Law no. 677/2001, as amended and completed. This way, the rule established by Article 7 paragraph (1) of Law no. 677/2001 on health related data is that such information is prohibited from processing. At the same time, processing such data is permitted in certain exceptional cases, expressly provided for in paragraph (2) of Article 7 of Law no.677/2001.

Therefore, personal data relating to state of health can be processed with the consent of the data subject or in cases of exception to the consent provided for in Article 7 and Article 9 of Law no. 677/2001.

Since the petitioner's address wasn't clear to the circumstances or context in which a physician would reveal data on the health of a patient to another doctor and the Medical College, he or she was given information about the procedure submitting a complaint to the National Supervisory Authority to protect the rights provided by Law no. 677/2001, in particular the right to information, access to data, intervention upon data, the right to object and not to be subject to individual decisions.

6. The National Institute of Statistics requested the National Supervisory Authority's opinion on the request of a police station, addressed to the institute, on the disclosure of data from documents produced in the Census of 2011, pursuant to Article 97 of the Criminal Procedure Code.

Law no. 677/2001 stated the conditions under which personal data may be processed, including disclosed. Under this legislation, the general rule governing the processing of personal data is the data subject's expressly and unequivocally consent.

Exceptionally, however, the personal data may be processed and disclosed by the data controller, without the consent of the data subject, in many exceptional cases. These cases, strictly interpreted, are expressly mentioned in Article 5 paragraph (2) of Law no. 677/2001, and among cases of exception to the data subject's consent include those where processing (disclosure) is required to fulfil a legal obligation of the data controller or to the performance of public measures or involving exercise public powers vested in the controller or the third party to whom the data is disclosed, and when the law expressly provides that, in order to protect an important public interest, with the condition that the processing is carried out with respect for the data subject and other guarantees provided by the law (Article 7 paragraph (2) letter h)) in conjunction with Article 8 paragraph (1) letter b).

In this context, the National Supervisory Authority also stated that according to the Law no. 238/2009 regulating processing of the personal data by the structures/units of the Ministry of Interior in the activities of prevention, investigation and counter crime and also maintaining public order,

republished, especially the Article 5, the police inspectorate must comply with the data collection and processing of personal data, without the consent of the data subject, to carry out research offenses.

At the same time, Article 53 of the Constitution provides that the exercise of rights or freedoms may be restricted only by law and only if necessary, inter alias, conducting a criminal investigation and the measure must be proportionate to the situation that caused it.

To ensure the data subject's rights, according to Article 16 of Law no. 677/2001, within the research activity of the offences, these carry a number of limitations, but only if that affects the efficiency of action or objective in carrying out statutory authority. These restriction situations are applicable only for the period necessary to achieve the pursued objective, and after the termination of that situation, measures will be taken for respecting the data subject's rights.

Consequently, the National Supervisory Authority stressed that personal data may be disclosed where there is not the consent of the data subject, under the statutory exception provided by Law no. 677/2001 in conjunction with Law no. 238/2009, meaning that it is necessary to analyze a determined case to respect the adequate, relevant and not excessive data character (i.e. strictly required for that purpose), framing the purpose of data request (or their disclosure) in one of the exception situations to consent, motivating the request, the data subject rights, etc.

The National Supervisory Authority has appreciated, in the context of the legal provisions mentioned above in relation to the contents of the address submitted, that the disclosure of the documents held by the National Institute of Statistics, "drafted in the Population and Housing Census in 2011 by a certain reviewer", to the police inspectorate, can be achieved respecting the conditions and safeguards laid down by the laws above.

E. Transmission/transfer of personal data

1. A polling institute asked for the National Supervisory Authority's point of view on the need for notification of processing operations and data transfer that they intend to carry out during a survey.

In regard to the raised issues, the National Supervisory Authority said that since the polling activity involves the processing of personal data, it falls under Law no. 677/2001, as amended and completed.

The data controller has been communicated the rules on the processing of personal data, including the one referring to obtain the consent of the data subjects and to inform them, as well as the applicable exceptions.

On loading the list of addresses of the persons interviewed on a server in Poland, the data

controller was informed that this activity is also a data processing operation and, in this situation, before loading that list, it is necessary to contact and to inform the data subjects. With regard to phone contacting the participants in the survey, the National Supervisory Authority drew attention to the need to respect the provisions of Article 4 of Law no. 506/2004 on the processing of personal data and privacy in the electronic communications sector, as amended, governing the conditions to be accomplished to ensure the confidentiality of communications and exceptional cases where it is permitted the recording, storing, any other form of interception or surveillance of communications and data traffic.

Finally, the data controller has been asked to update the information stated in the notification form, especially since the data from surveys are intended to be stored on a server in Poland.

2. A law firm addressed the National Supervisory Authority on the situation of a company in Romania, part of a multinational group, which will implement an online and phone reporting system, through which its employees notify "various violations of the rules of conduct in society or of the law (Whistleblowing Hotline)" to the mother -company of a Member State of the European Union.

Related to the above, the National Supervisory Authority held that, in the implementation of "Whistleblowing Hotline" the society from Romania must fill up a notification to register the processing of personal data in electronic register hold by the Authority or to complete/modify one already made, as appropriate.

The content of the reply stated that the processing of personal data via the "whistleblowing" is part of the terms of Decision no. 11/2009 of the National Supervisory Authority, so that it could be performed a prior control in this case.

II. Applicability of Decision no. 52/2012

1. A city hall sought a point of view on the processing of personal data of employees, carried out by video surveillance means in offices where they work.

With regard to the employee's personal data processing by video surveillance means, inside the offices where they work, it is allowed only in cases provided by law or based on the opinion of the national supervision.

As such, video surveillance is prohibited inside the office, unless expressly provided for in a law that obliges the employer to establish video surveillance systems (e.g. Buildings banks) or those authorized by the National Supervisory Authority under Article 8 paragraph (3) of Decision

no. 52/2012, in duly justified cases.

In the context of the above, the need to ensure effective protection of the right to privacy of employees, based on respect for the principle of proportionality processing of personal data, the situation presented on video monitoring employees within the offices of the institution in terms not invoking relevant rules, the National Supervisory Authority has appreciated steadily that such processing is excessive to the purposes stated, and is likely to affect their privacy.

2. A goods transport company has applied for a waiver from the 30-day storage of personal data obtained through video surveillance system established by Article 14 of the Decision no. 52/2012 of the National Supervisory Authority, for the purposes of its extension.

The response stated that the processing of personal data by the use of video surveillance is subject to both the provisions of Law no. 677/2001 the protection of individuals with regard to the processing of personal data and on the free movement of such data, as amended and supplemented, Decision no. 52/2012 concerning the processing of personal data through the use of video surveillance and the Law no. 333/2003 on guard, goods, valuables and personal protection, as amended.

According to Article 14 paragraph (1) of Decision No. 52/2012, the period of the retention of the data obtained through video surveillance system should be proportionate to the purpose for which the data is processed, but no more than 30 days, unless expressly regulated by law or duly justified cases.

In regard to the details of the obligation of the business, as a member of the Association for the Protection of Goods Transported (TAPA) to keep the images collected by video surveillance system on a minimum of 30 days, the Supervisory Authority found that it is not required to assess the granting of an exception to the term storage provided by Decision no. 52/2012.

III. Applicability of Law no. 238/2009

The Inspectorate for Emergency Situations of Caraş - Severin requested clarification regarding whether to notify the processing of personal data that they carry out within the purposes of finding and sanctioning offences, in fulfilling its statutory duties.

For the purposes of Article 3 letter e) of Law no. 677/2001, the data controller is any natural or legal person, private or public law, including public authorities, institutions and their territorial entities, which determines the purposes and means of processing personal data. Also, if the purpose and means of processing personal data is determined by a law or under an enactment, the data controller is the legal entity of public law, which is designated data controller by that law or under that Act.

At the same time, by the provisions of Article 1 in conjunction with Article 4 of Law no. 238/2009 it was established the obligation for the structures/units of the Ministry of Interior to notify the National Supervisory Authority the processing performed for the above mentioned purposes.

Accordingly, to the points made in relation to Article 1 of the Government Ordinance no. 88/2001 on the establishment, organization and functioning of public services for emergency situations, as amended and supplemented, under which the professional services are considered under the General Inspectorate for Emergency Situations, specialized body of the central government under the Ministry of Interior, has announced that the Inspectorate for Emergency Situations of Caraş-Severin has an obligation to notify the National Supervisory Authority the data processing performed in order to ascertain and punish offenses.

Section 3 The representation activity before courts of law

The solutions delivered by the courts of law during the year 2013, in the litigations on their roles, confirm the existence of an approach and interpretation similar to that of the National Supervisory Authority on specific regulations applying to the protection of personal data.

Regarding the object of the promoted actions before the courts of law, most of them were focused on the failure of notification, unlawful processing of personal data by retaining copies of identity documents, by video surveillance means, but also by the disclosure of personal data to a large public and also forwarding of unsolicited commercial messages in violation of the Law no. 506/2004.

The following are some of the relevant circumstances in which sanctions were contested by the National Supervisory Authority:

1. Unlawful processing of personal data by retaining copies of identity documents

The National Supervisory Authority conducted an investigation to a data controller, as a result of a complaint relating to the retention of a copy of an identity card.

The representatives of the National Supervisory Authority found that the data controller had contracts concluded with the customer to provide certain services, i.e. internet, cable TV, fixed and mobile phone. From their content does not result the client's consent to withhold copies of ID card when purchasing a product that was related to one of the contracts.

The documents provided by the data controller to the National Supervisory Authority representatives revealed that the data controller processed the personal identification number of his clients without notifying such processing.

The processing of personal identification number was carried out by the data controller without the express and unequivocal consent of the client or an express legal provision that would allow the collection or the existence of an authorization from the National Supervisory Authority, as stipulated expressly Article 8 of Law no. 677/2001 and Article 2 of Decision no. 132/2011.

The offences committed by the data controller as incomplete notification and unlawful processing of personal data by retaining a copy of the applicant's identity card without its express and unequivocal consent were sanctioned with a fine.

The data controller has filed a complaint to a court of law against the report of finding/sanction entered the National Supervisory Authority.

The court ordered maintenance of the penalty imposed by the National Supervisory Authorities, by irrevocable decision.

2. The processing of personal data by video surveillance means

In exercising control competences the National Supervisory Authority ordered an investigation following a complaint relating to the installation of video cameras in all offices of the data controller's employees.

During control it has been found that the data controller had bought a video surveillance system that was put into service in late November 2012. This system was composed of cameras located throughout the property, including inside the offices.

On the same occasion, the data controller declared that the purpose of the mounting of the system would have been the safety of the employees, due to the fact that there were some unexpected events.

It was also noted that the data controller collected images of employees in offices without the existence of a legal provision allowing such an operation.

At the same time, the data controller was collecting data on all persons entering/exiting the building, without this activity been notified to the National Supervisory Authority. It was also found that the data subjects had been only partial informed of this, only in the halls of the building.

Therefore, the data controller has committed offences provided by the law, consisting of failure to notify and unlawful processing of personal data, which were fined by the National Supervisory Authority.

The data controller has filed a complaint against the report of finding/sanction entered the National Supervisory Authority.

The court of law, analyzing the evidence given in the case, held that the data controller failed to

notify data processing consisting of images collected by video surveillance system installed. At the same time, the court found that the data controller did not provide full information and appropriate subjects on the data processed.

The court held that the data controller is found guilty of committing offences, but in terms of actual penalty imposed, the court held that the offences committed by the data controller pose a low threat to society, so he decided to replace the fine with a warning.

The court decision is irrevocable.

3. The disclosure of personal data to the public

In exercising the control functions, the National Supervisory Authority ordered an investigation following a complaint relating to the disclosure of personal data over the Internet by a public institution.

This disclosure was produced by attaching the complaint of the complainant to an address sent to a third party. The latter has published on a website the petitioner's complaint, which contained more personal data (name, address and personal identification number).

The right of intervention upon the data held by the provisions of Article 14 of Law no. 677/2001, the petitioner addressed a public institution that originally revealed its data, but its efforts remained fruitless.

To resolve such issues, the National Supervisory Authority ordered an investigation at the data controller's premises. Thus, it was requested to provide additional information concerning the information sent on the petitioner, in advance, on issues relating to the transmission of personal data to a third party, the purpose of the disclosure of the data and how the complaint of the petitioner was resolved.

The documents made available by the data controller revealed that the data controller has notified the third party about the petitioner's complaint, without obtaining its prior express and unequivocal consent.

Also, after analyzing the documents provided by the data controller, it was also found that the petitioner did not respond to a request under Article 14 of Law no. 677/2001.

The acts committed by the data controller were sanctioned with a fine, and the data controller has filed a complaint against the report of finding/sanction entered the National Supervisory Authority.

The court of law found that the report was legally drafted, the contravention sanctions imposed by the National Supervisory Authority were maintained, and the decision became final.

4. The transmission of unsolicited commercial messages

In exercising control attributions, the National Supervisory Authority ordered an investigation following a complaint regarding the transmission of unsolicited commercial message which includes offers of products of a data controller.

Following the aforementioned complaint, additional data was required from the data controller's internet provider, who confirmed that the IP address from which the message was sent was allocated to this data controller in the date and time indicated by the National Supervisory Authority.

During the investigation, it appeared that the data controller transmitted to clients/potential clients commercial communications of the products it marketed.

Regarding the transmission of electronic messages advertising, Directive no. 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector requires, in principle, the user's prior consent to receiving such messages.

Directive no. 95/46/EC and Law no. 677/2001 impose on the data controller's personal data certain obligations, such as the notification of data processing by the Supervisory Authority, the information and ensuring the confidentiality and security of processing.

At the same time, Article 12 paragraph (1) of Law no. 506/2004 on the processing of personal data and privacy in the electronic communications sector, requires the prior consent of the subscriber (how opt-in) in the relationship between the participants in direct marketing and Internet users. According to this article, " commercial communications through the use of automated calling and communication systems that do not require human intervention, by fax or by electronic mail or by any other method that uses publicly available electronic communications services, unless the subscriber or user concerned has given his prior express consent to receive such communications is prohibited."

In the same investigation, the data controller's representatives admitted that the commercial message received by the petitioner was sent by the data controller, although it did not expressly consent to receive such communications.

Consequently, it was found committing the offence provided for in Article 13 paragraph (1) letter q) of the Law no. 506/2004, as data controller of commercial messages sent to the complainant by e-mail, although it did not expressly consent to receive such communications, the data controller being fined.

The data controller has filed a complaint against the report of finding/sanction entered the National Supervisory Authority, requiring replacement of the fine sanction the warning.

The final ruling, the court of law dismissed the complaint filed by the data controller, showing

that the sanctions of the fine are justified in relation to the seriousness of the offense and the effects produced.

Section 4 Public Information

During 2013, the National Supervisory Authority continued communication activities designed to inform the public about the specific rules of protection of personal data.

Among the significant events in which our institution was involved, we highlight:

- The Ro-Direct Conference organized by the Romanian Association of Direct Marketing—ARMAD, from 7 to 8 November 2013 in Bucharest, where the National Supervisory Authority representatives have presented "Processing and protection of personal data in direct marketing";

- The debate on "Open data and personal data: the search for a compromise needed" organized by the Soros Foundation Romania and the Association for Technology and Internet on 2013 November 29, in Bucharest. During the event, representatives of the National Supervisory Authority gave presentations entitled "Protection of personal data for the use of open data."

At the same time, the information provided by telephone and during audience program at the National Supervisory Authority was done quickly and efficiently, informing citizens and data controllers, in the meaning that were offered, in a direct manner, useful information on rights of data subjects and obligations of data controllers' clarification on the conditions of processing and disclosure to third parties.

Through its website www.dataprotection.ro, our institution has sought to ensure adequate information to individuals and data controllers may contact us using the email address including: anspdcp@dataprotection.ro.

Considering the importance of the publication by the European Commission proposal for a Regulation, which is part of the reform package on the protection of personal data, the communication activity of the National Supervisory Authority was focused on the public debate of these documents, as well as on the inter-institutional cooperation , at a national level, for preparing Romania's position within Dapix Working Group of the Council of the European Union, established to analyze the mentioned legal package.

The interest of the media to the protection of personal data was reflected in newspaper articles published on various topics involving the proper use of personal data. Print media has sought the views of the National Supervisory Authority and reflected its business, particularly investigations conducted and measures taken.

In order to popularize the work of the institution and specific regulations in the field, on the

website www.dataprotection.ro have been published press releases that were reported significant aspects of control activities or other events in which was involved the National Supervisory Authority.

The press releases or the responses to requests from the media resulted in several articles that have brought public attention to our institution's position regarding the conditions of disclosure of personal data, the rights of citizens in this area (in particular the right to information and the right to file a complaint), the possibilities of recovery and the role of the Supervisory Authority.

We are convinced that the media will continue to be an important support to the work of our institution in order to inform the public about the rules of use of personal data.

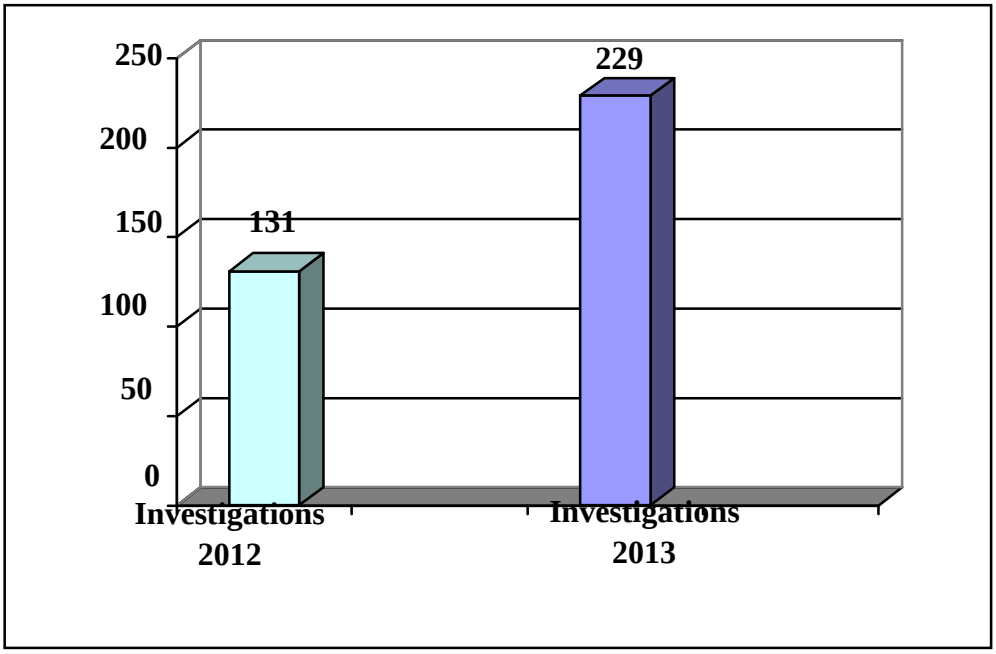
CHAPTER IV
THE CONTROL ACTIVITY

Section 1: Overview

The monitoring and control activities carried out by the National Supervisory Authority in 2013 were influenced by budgetary constraints and economic circumstances related to blocking positions, so that of ex officio investigations were planned mainly in the municipality of Bucharest and the surrounding counties, granting priority to the inspections conducted for handling complaints and notices. For some investigations requiring travel to remote areas of the country, the written procedure for obtaining the information necessary to resolve matters raised was followed and where necessary, by penalizing data controllers and issuing recommendations.

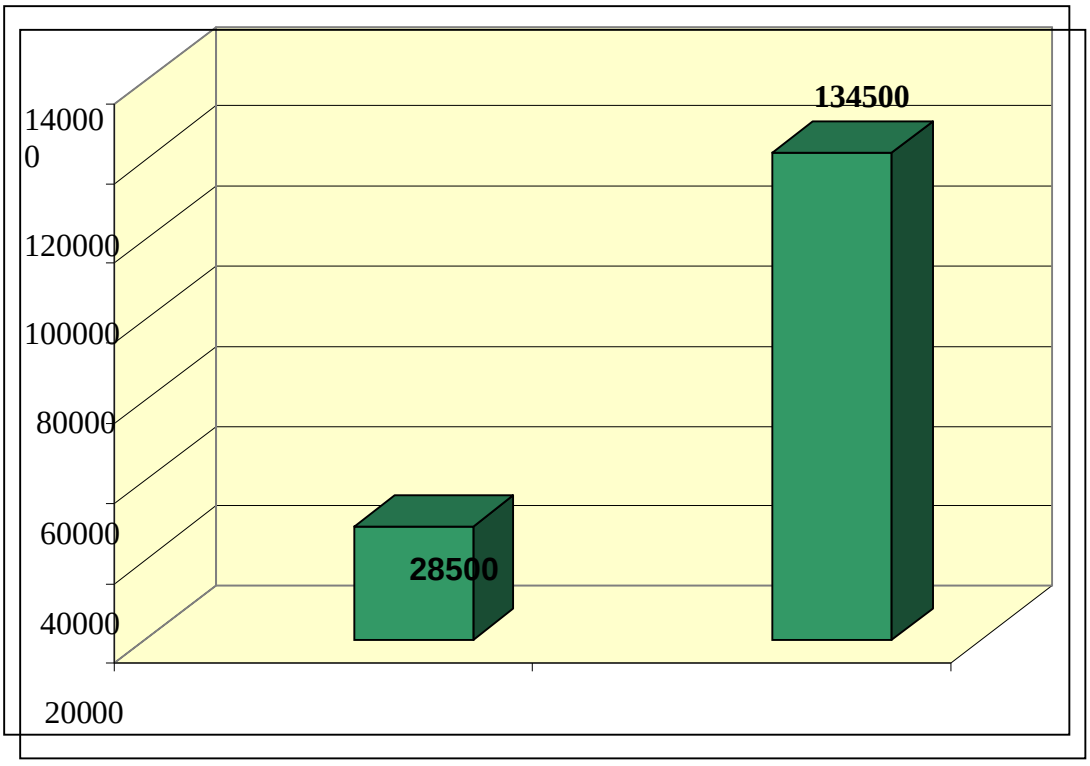
Thus, in 2013, a total of 229 control actions were performed on site, including 78 ex officio controls and 151 controls to settle the 877 complaints and notices sent the National Supervisory Authority, an increase in comparison to the previous year. Also, in order to answer complaints and notices, a total of 44 investigations were carried out in writing.

Figure 1: Number of controls 2012-2013



Following the controls carried out, contraventional sanctions were imposed consisting of 66 fines and 124 warnings. **The total amount of fines imposed is of 134,500 lei, up by over 300% from 2012.**

Figure 2: The amount of the fines imposed in 2012-2013



In accordance with the provisions of Article 21 paragraph (3) letter d) of Law no. 677/2001 and Article 3 paragraph (5) of Law no.102/2005, in cases where the provisions of Law no. 677/2001 were breached, depending on the circumstances, in addition to sanctions for offenses, certain mandatory measures were ruled, through decisions or recommendations of the president of the National Supervisory Authority.

In this context, 5 decisions were issued to delete personal data processed, one decision to terminate the processing of personal data and to delete the processed data and one recommendation.

Section 2: Ex Officio Investigations

During the year 2013, a total of 78 ex officio control actions were performed on site.

Most ex officio investigations have concerned the observance of the provisions of Decision no. 132/2011 issued by the National Supervisory Authority on the conditions of processing the personal identification number and other personal data having a generally applicable identification function.

Other ex officio investigations were performed as a result of certain notices sent by personal data controllers, as well as a result of articles emerging in the press, in the following areas:

1. The processing of personal data of employees through a computer application for monitoring their working time;

2. The processing of personal data of employees in order to install and use a biometric authentication system;

3. The processing of the personal identification number and other generally applicable identifying data;

4. The disclosure of personal data of the victim of a criminal act, in a press statement.

The total amount of fines imposed in ex officio investigations was of 12,500 lei.

I. Compliance with the provisions of Decision no. 132/2011 on the conditions of processing the personal identification number and other personal data having a generally applicable identification function

The controlled entities were department stores (hypermarkets, shops selling furniture or plumbing etc.), banks, exchange offices, local public transport authorities, local police and companies lifting illegally parked vehicles.

The National Supervisory Authority has verified if investigated data controllers have requested copies of identity documents and other documents containing information protected by Article 8 of Law no. 677/2001 (ID card, passport, birth certificate, driving license) in cases in which the legal conditions set out in Article 8 of Law no. 677/2001, reiterated in Article 2 of Decision no. 132/2011 were not met. It was also verified if such personal data (contained in those documents) was collected excessively, without being necessary for fulfilling the declared purposes of the processing or if they are stored excessively, without setting limited periods.

According to Article 8 of Law no. 677/2001, the processing of the personal identification number and other generally applicable identification details is permitted only under the following conditions:

- The data subject has given his/her express consent;
- The processing is explicitly provided by a legal regulation;
- In other cases established by the supervisory authority, provided that adequate safeguards for the rights of data subjects are set up.

These conditions are also set out in Article 2 of Decision no. 132/2011 concerning the conditions of processing the personal identification number and other personal data with a generally applicable function of identification, issued by the National Supervisory Authority. The decision exemplifies such data within Article 1 paragraph (1): personal identification number, series and number of identity card, passport, driving license, social or health security number.

In accordance with Article 6 of the Decision, the collection and processing of such data, including their disclosure, by making and retaining copies of the ID card or the documents containing them, are prohibited, except for the cases provided in Article 2.

1. Thematic investigations performed at major stores (hypermarkets, hardware store, furniture retail etc.)

Major stores process only personal data from the category protected by Article 8 of Law no. 677/2001 (personal identification number, series and number of identity card) as data

controllers. They process data in order to fulfil their obligations to manage HR activities, the purpose of issuing invoices and the purpose of commercials, marketing and advertising.

Upon inspection it was found that: data controllers investigated by the National Supervisory Authority have submitted incomplete notifications (not all purposes of processing data have been declared), some of them excessively collect and process personal data with identification function belonging to the category protected by Article 8 of Law no. 677/2001, they not provide complete informing to data subjects in accordance with the provisions of Article 12 of Law no. 677/2001.

Considering the issues mentioned above, sanctions were applied on the data controllers and it was recommended that they complete the previously submitted notifications, draw up procedures to establish limited periods of storage, as well as rules relating to destruction/deletion of personal data, including the copies of documents containing them, which shall also include the future destination of the data according to Article 6 of Law no. 677/2001, as well as to inform the data subjects in accordance with the provisions of Article 12 of Law no. 677/2001. Also, in certain cases, measures have been imposed to limit the collection and processing of data with identification function such as personal identification number, series and number of the identity card.

CASE FILE

During an investigation of a data controller operating in the field of retail furniture, lighting equipment and other household articles, in specialized stores (supply of goods and services), the following findings were made:

The investigated data controller, although it has notified the National Supervisory Authority of the personal data processing, prior to the investigation, has not declared all the purposes for which the personal data were processed, also no mention was made in the notification form of the fact that the data controller was transmitting these data to the European Union. Also, it was found that it was excessively collecting and processing the personal identification number of its customers for the purpose of issuing invoices, although they were not part of the category of persons paying tax or VAT.

According to Article 155 paragraph 19 letter f) of the Tax Code, as amended, the name / name and address of the beneficiary of the goods or services, as well as the registration code for VAT or tax identification code of the beneficiary must also be among the

information required to be included in the invoice, if it is a taxable or non-taxable legal person.

Since, in most cases, individuals are non-taxable persons, it was appreciated that it is not compulsory for invoices for this category of data subjects to contain their personal identification number.

In regard to the findings, it was recommended to the data controller to complete the relevant sections of the notification recorded in the Register of personal data processing, to modify the used application in order to eliminate the field concerning the personal identification number and to further meet the provisions of Decision No. 132/2011 concerning the conditions of processing the personal identification number and other personal data with identification function of general applicability.

The data controller has received a contraventional sanction, for the offense referred to in Article 31 of Law no. 677/2001, for incomplete notification and for the offense referred to in Article 32 of Law no. 677/2001, meaning the unlawful processing of personal data as a breach of Article 4 letter c) of the same Law, in relation to Article 2 of Decision no. 132/2011, since the data controller has excessively collected and processed the personal identification number of customers who are not part of the category of persons paying tax or VAT.

CASE FILE

Another investigation was conducted at a hypermarket which has notified the processing of personal data for purposes of commercials, marketing and advertising.

Following the checks carried out during the investigation, it was found that in the regulations drawn up by the hypermarket for its contests it was mentioned that, at the moment of the taking over the prize, the winners of the contest must draw up an affidavit which also serves to collect their ID card's series and number.

The data controller's representatives have stated that, although personal data with identification function were collected to verify the winners, so that they will not be found in one of the cases of incompatibility set out in the contest rules, ultimately no checks were carried out, except concerning its own employees. Thus, the human resources department has not carried out checks on the quality of 1st and 2nd degree relatives of the employees, but rather checks on whether or not they are employees of the said hypermarket.

In regard to the aforementioned situation, the inspection team has judged that the

collection of the ID card series and number through the affidavit made by the winner, in order to determine incompatibilities, is not justified.

It was also found that the data controller had stated in the rules and regulations of the contests that it will publish the name, surname and city of domicile / residence of the winners on its website, although the Government Ordinance no. 99/2000 stipulates the obligation of the organizer to publish only the name of the winners and the winnings awarded.

The data controller has been sanctioned for committing the offense provided by Article 32 of Law no.677/2001, having processed the series and number of the ID cards since 2011 and until the date of the inspection for marketing and advertising purposes, in breach of the provisions of Article 4 letter a) and c) and Article 8 of Law no. 677/2001, excessive processing in relation to the purpose of collection and further processing of such data.

It was also recommended to the data controller to remove the series and number of the ID card from the affidavits of the winners and to update the notification form.

2. Thematic investigations conducted in banking institutions

During the controls conducted in banking institutions, it was verified if they require copies of identity documents and of other documents containing information protected by Article 8 of Law no. 677/2001 (personal identification number, series and number of identity document, passport, driving license, social or health security number) in cases where the legal conditions stipulated by Article 8 of Law no. 677/2001 are not met, and if such personal data (contained in those documents) are excessively collected, without them being necessary for the stated purposes of the processing or if they are excessively stored, without setting limited periods.

Pursuant to the inspections, it was discovered that banks collect and retain copies of identity documents and of other documents containing information protected by Article 8 of Law no. 677/2001, by invoking the provisions of Article 8 paragraph (2) and Article 22 of the National Bank of Romania (NBR) Regulation no. 9/2008 for the purpose of verifying customer identity (standard "know your customer" measure), pursuant to the provisions of Article 13 paragraph (1) of Law no. 656/2002.

In accordance with Article 8 paragraph (2) from the NBR Regulation no. 9/2008, verifying the customer's identity (as a standard "know your customer" measure) is based on

documents belonging to the category of most difficult to counterfeit or to obtain unlawfully or under a false name, such as identity documents issued by an official authority that includes a photograph of the holder. Also, according to Article 22 of the same Regulation, pursuant to Article 13 paragraph (1) of Law no. 656/2002 ("in every case where identity is required under the provisions of this law, the legal or natural person referred to in Article 8, which is required to identify the customer, will keep a copy of the document as proof of identity, or references of identity, for a minimum period of five years from the date when the customer relationship ends"), institutions are required to keep at least copies of identity documents of individuals.

According to Article 9 paragraph (1) of Law no. 656/2002, persons referred to in Article 8 are required to apply standard "know your customer" measures in the following situations:

a) when establishing a business relationship;

b) when carrying out occasional transactions amounting to at least EUR 15,000 or equivalent, whether the transaction is carried out in a single operation or in several operations which appear to have a connection between them;

c) when the transaction is suspected of money laundering or terrorist financing, regardless of the scope of provisions derogating from the obligation to apply standard "know your customer" measures established in this law and of the value of the transaction;

d) if there are doubts about the veracity or relevance of the identification data previously owned concerning the customer;

e) when purchasing or exchanging chips in casino whose minimum is the RON equivalent of EUR 2,000.

It was found that the investigated banking institutions have established procedures on requesting and retaining copies of identification document and documents containing data with identification function, as well as concerning the periods of their storage.

Upon the undertaken inspections, it was found that the investigated banking institutions do not retain copies of identity documents and other documents containing information protected by Article 8 of Law no. 677/2001, except in cases provided by law.

III. Thematic investigations conducted at companies that lift illegally parked vehicles

From the investigations carried out in such companies, having as main activity the

lifting of illegally parked vehicles, it was found that they process personal data from the category protected by Article 8 of Law no. 677/2001 only as warrantees of the local councils, with the rules on collection, transport, storage and release of vehicles parked illegally on public domain and which constitute an obstacle to public traffic being provided in the decisions taken by the local councils.

The activity of the companies that lift illegally parked vehicles is conducted under a service concession agreement concluded with the local police, which are subordinated to the local councils. These companies perform specific operations based on a written mandate for lifting signed by the local police officer.

Recovery of vehicles by their owners is made based on presenting their identity card, driver's license and vehicle registration form, in original, at the local police office where an offense report will be filled in.

After paying the fee at the vehicle lifting company's cashier, the vehicle owner goes to the public relations' agent to recover the vehicle, with the latter drawing up a fact-finding report in two copies, of which one is sent to the local police.

The fact-finding report is a standard form established by the district councils, in which a data sheet of the vehicle and personal information about the holder are completed: name, signature and personal identification number.

IV. Thematic investigation performed at local police stations

From the investigations conducted, it was found that local police are processing personal data as data controllers.

Each local police has its own Rules of organization and operation, and procedures that set forth rules on conducting the activities of lifting, transportation, storage and release of parked vehicles and stray or abandoned vehicles on land belonging to the public / private sector.

For lifting vehicles that are found to be parked abusively / illegally, the lifting disposition and fact-finding report are prepared on the spot by the traffic officer. These documents help to collect only the make, model, colour, location and physical condition and the license number of the vehicle.

The representatives of investigated local police have declared that copies of the

identity card are only requested in the following situations:

- Where the owner receives the vehicle lifting disposition and notice by post, he/she can send documents to the Police proving his/her identity, including a copy of the identity document, on his/her own initiative;

- Where a car was lifted and the person who has received the lifting disposition and notice is no longer the vehicle's owner, he/she may send a copy of his/her identity card and of the sale-purchase agreement of the vehicle to the Police, on his/her own initiative.

In the internal Regulations there is no reference to keeping the copies of identity documents and other documents containing information protected by Article 8 of Law no. 677/2001, while the statements of the data controllers revealed that such copies are not required to perform the activity of lifting, transportation, storage and release of parked vehicles and stray or abandoned vehicles on land belonging to the public / private sector.

II. Ex officio investigations as a result of analyzing certain notifications submitted by personal data controllers and of certain articles in the press

1. The processing of personal data of employees through a computer application for monitoring their working time

CASE FILE

A public institution has decided to monitor the working time of employees through a software application installed on their workstations.

Following the checks carried out on the premises, it was found that the public institution was processing the personal data of their employees in order to monitor, through automated means, the applications used and websites visited in order to determine the productivity of each employee.

The software application, installed by a company who was acting as a proxy, allowed monitoring the correct operation, from a hardware and software perspective, of the workstations of employees, volume and names of the printed documents, used applications and websites, as well as usage times of the systems. This application generated reports containing the user's name and surname, the specific code of the user's department, computer number, time of opening and closing the computer, productivity expressed as a percentage,

time considered to be productive, idle time, work time.

The used software was transmitting information from each workstation to the servers of the company that owned the application, located in the United States.

Considering the above, it was found that:

- the data controller did not notify the processing of personal data of their employees for monitoring purposes, through automated means, concerning their use of applications and access of websites, including transfer to the USA and processing excessive data of the employees in relation to the purpose for which they were collected;

- The data controller has not provided evidence of adequately and completely informing the employees regarding the purpose for which the data processing was performed and the recipients of the data;

- The contract concluded with the company empowered to data processing carried out by means of the software did not contain the clauses required by Aricle. 20 paragraph (5) of Law no. 677/2001;

- The data controller processed personal data by means of a video surveillance system as well, an operation that was not notified to the National Supervisory Authority.

As such, the data controller has been sanctioned for the offenses referred to in Article 31 of Law no. 677/2001, Article 32 of Law no. 677/2001 and Article 33 of Law no. 677/2001.

2. The processing of personal data of employees in order to install and use a biometric authentication system

CASE FILE

A banking institution decided to use a biometric authentication system for their employees, following the detection of certain fraudulent acts.

The biometric authentication system used by the banking institution implied the enrolment of the thumbs' dermatoglyphs from both hands. They are only stored in the biometric authentication device that is non-transferable equipment kept by the user (employees). Fingerprints are not stored in a central database or locally. Upon termination of employment of an employee, the biometric device is reset, which irreversibly deletes private biometric information and resets the device to the factory settings provided by the manufacturer.

The employees were informed and signed an agreement concerning the use and processing of personal data in view of enrolment to the biometric authentication system.

At the same time, at the level of the banking institution information security procedures were established relating to the implementation of biometric authentication.

Considering the above, it was found that the biometric authentication system used by the controlled banking institution complied with the general rules on the processing of personal data provided by Law no. 677/2001.

3. The processing of personal identification number in advertising lotteries

CASE FILE

In an investigation carried out in the territorial branch of a political party, excessive processing of the personal identification number of participants to an advertising lottery was discovered, in relation to the purpose for which it was collected and subsequently processed.

To organize a raffle, the data controller established, through the Regulation concerning its organization, that the raffle tickets will contain references to the name and surname, address, phone and e-mail of the participant.

After the conducted inspection, it was found that the lottery tickets also contained other personal data than those laid down in the Regulation of the raffle, specifically the personal identification number.

The data controller has been sanctioned for committing the offense provided by Article 32 of Law no.677/2001, since it has processed the personal identification number of the participants in the raffle without their express consent, without the processing being expressly provided for by a legal provision or without having the endorsement of the National Supervisory Authority in this respect, which is in breach of Article 8 of Law no. 677/2001 and Article 2 of Decision no. 132/2011 concerning the conditions of processing the personal identification number and other personal data with a generally applicable identification function.

4. Disclosure of personal data of the victim of a criminal act, in a press statement

CASE FILE

A prosecutor's office disclosed personal data of the victim of a criminal offense without his consent, in a press statement issued by the spokesman of the institution.

The press release was distributed at the same time at a television newscast, while the video of the statement was posted on the broadcaster's website, which could be accessed by any visitor to the site.

The data controller representative stated that, at the time of the interview, the spokesman quoted from material prepared according to the report of the facts of the case, where the victim's full name appeared. In the press release issued later, identification data of the victim in the case was made to be anonymous by using initials.

The data controller was fined for the offense provided by Article 32 of Law no. 677/2001 for breach of Article 5 of this law.

It was also recommended to the data controller to draw up a document showing that it has conducted trainings for its spokesmen, concerning the protection of personal data of data subjects in relation to mass media.

Section 3 The activity of settling complaints and notices

1. Overview

While undertaking the powers provided by law, the National Supervisory Authority has received and settled, during 2013, complaints and notices relating to the processing of personal data in various fields, a considerable number regarding the financial-banking, electronic communications and online environment sectors, as well as the monitoring and security of the public or private spaces by means of video surveillance. In each of these areas different topics of complaints and notices were identified, according to the issues claimed by the petitioners.

Thus, in the field of finance-banking, where data controllers are mainly banks and non-bank financial institutions, petitioners notified mostly about the reporting of personal data to credit office type filing systems, disclosure of personal data to debt recovery companies or processing of personal data by retaining copies of identity documents. Pursuant to the investigations conducted, it was found that data controllers have not complied with the provisions of Law no. 677/2001 and of the Decision issued by the National Supervisory Authority no. 105/2007 on the processing of personal data carried out in credit bureau type filing systems, in terms of the deadline for transmitting data to the credit bureau, the period of prior notice to the data subjects, forwarding a response within 15 days to the complainant's request to exercise the rights provided by Law no. 677/2001.

A significant share of the total number of complaints registered in 2013 is represented by complaints and notices covering electronic communications and the online environment. The petitioners complained, mostly, in regard to the transmission of unsolicited commercial messages, sale of e-mail databases and the disclosure of personal data on the Internet. In this vast area of activity, the accused data controllers are mainly companies operating online trading activities, travel agencies as well as telephone and Internet service providers. Following the undertaken investigations, it was noted that the personal data of the data subjects were processed without their consent and the requests to exercise the rights of the data subjects were not pursued, especially the right of opposition that targeted deletion of the data.

Unlike previous years, there was a significant increase in complaints and notices covering the processing of personal data by means of video surveillance, in most cases the

accused data controllers being owners' associations. However, petitions by which the National Supervisory Authority was informed about the processing of data carried out by means of video surveillance systems by schools, city halls, trading companies or individuals were not missing. Pursuant to the investigations conducted, it was found that the data controllers are not aware and do not comply with the applicable legal provisions on data processing by means of video surveillance (Law no. 677/2001 and Decision No. 52/2012 concerning the processing of personal data by use of video surveillance), especially those regarding the rights of data subjects, the conditions in which the processing of images may be performed, notifying the processing to the National Supervisory Authority.

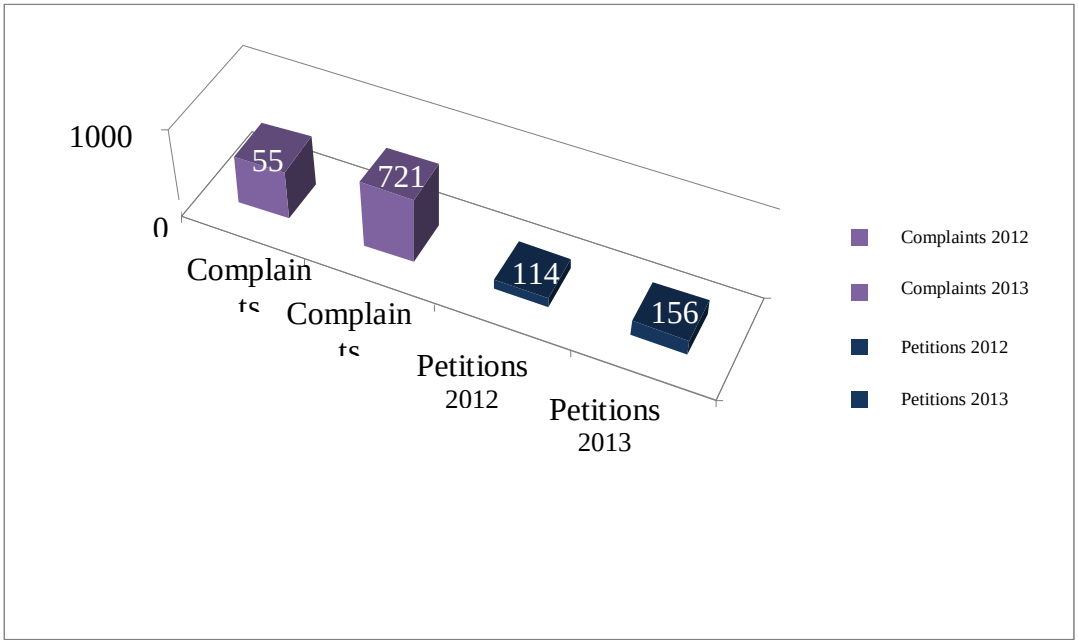
In the cases considered to have grounds sanctions for offences were applied and, where appropriate, measures to stop, delete or suspend the processing of personal data were ordered.

Regarding the inadmissibility of petitions received, in 2013, the main reason for rejecting complaints remains the failure to meet the prior legal procedure by petitioners. Thus, the provisions of Article 25 of Law no. 677/2001, providing that the complaint to the National Supervisory Authority cannot be forwarded earlier than 15 days after filing a complaint with the same content to the data controller, are not followed. To remedy this situation, in the second part of 2013, the section on the procedure for submitting a complaint and the templates that can be used by those interested has been amended, in order to increase the visibility of this information on the website of the National Supervisory Authority (www.dataprotection.ro). At the same time, our institution has posted the procedure and forms for submitting a request for access and / or intervention / amendment, deletion or blocking of personal data stored within USA Tracking Program of Terrorism Financing, in accordance with the Agreement between the United States and the European Union on the processing and transfer of financial messaging data from the EU to the United States in the Terrorism Financing Tracking Program, on its website.

Other reasons for rejecting complaints submitted by data subjects as being inadmissible or unfounded were: failure of providing evidence to support the complaint, noticing of issues for which the National Supervisory Authority has no material or territorial jurisdiction to intervene, the precise identification of the accused entity was not possible (i.e. the sender of unsolicited electronic commercial communications) or the prior introduction of a legal action before a court of law.

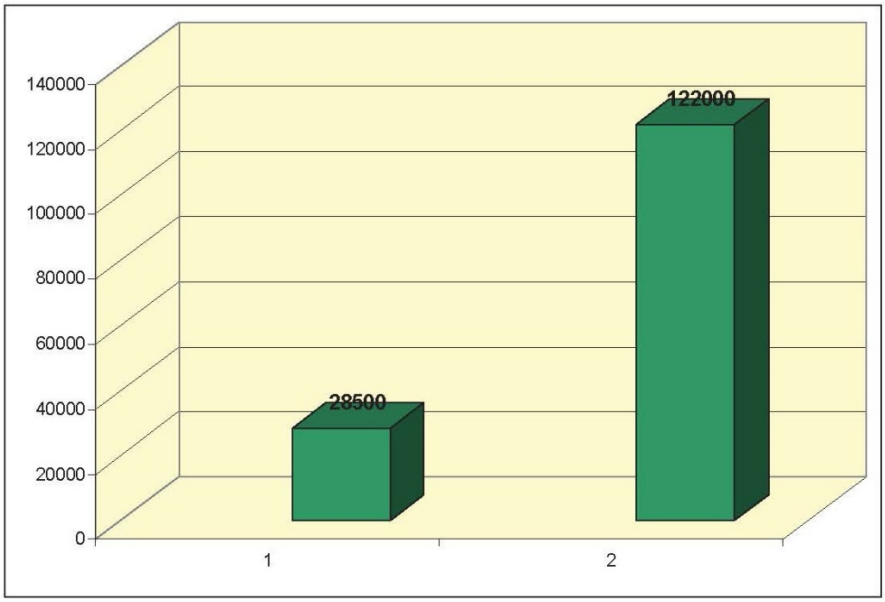
During 2013, The National Supervisory Authority has received a considerable number of complaints, compared to the previous year, specifically 721 complaints, 156 notices.

Figure 1: The number of complaints and notices in 2012 - 2013



For the settlement of complaints and notices received, 151 on the spot investigations and 44 inquiries in writing were performed, pursuant to which sanctions were applied consisting of 61 fines and 119 warnings. The total amount of fines imposed in 2013 under investigations performed for the settlement of complaints and notifications is of 122,000 lei, up by over 300% compared to 2012.

Figure 2: The amount of the fines imposed in the settlement of claims and complaints in 2012-2013



Moreover, 5 decisions to delete personal data processed were issued, one decision to terminate the processing of personal data and deletion of data processed and one recommendation.

II. The main findings resulting from the settlement of complaints and notices

1. Processing of personal data by retaining copies of identity documents

In 2013, the number of complaints and notices addressed to the national supervisory authority which helped to report breaches of legal provisions concerning the processing of personal data by retaining copies of identity documents has increased. Pursuant to the investigations carried out, it was found that the accused data controllers have not requested an endorsement from our institution, prior to the introduction of the procedure for collecting copies of identity documents, as required by Decision no. 132/2011 regarding the conditions of processing the personal identification number and other personal data with a generally applicable identification function, in those cases where there was no evidence of the consent of the data subjects or the existence of a law allowing the collection of copies of identity documents.

CASE FILE (public transport companies)

During 2013, several petitioners addressed the Supervisory Authority claiming that, since April 2013, a public transport company has conditioned the recharging of subscriptions issued with exemptions or reductions on different grounds, by getting scanned copies of the identity documents and other documents of the beneficiaries. The petitioners have claimed that earlier to this date, the transport company did not store copies of identification documents.

Pursuant to the investigation, it was found that the scanning of identity documents and other supporting documents that are proof of receipt of subscriptions at reduced rates was decided, as follows:

- For students: valid student card, birth certificate / identity card / passport / residence card, marriage certificate / court order or other acts issued public institutions;

- For pensioners residing in the province: pension slip, ID card, marriage certificate / court order / other acts.

These documents were requested at card issuance and recharge centres, at the time of first issue of the subscription card, at the beginning of school / university or when changes occur that do not emerge from the submitted documents.

The data controller's representatives argued that before applying this procedure, a copy of the ID card and of other supporting documents was requested.

The data controller's representatives argued that the scanning procedure was used to reduce fraud in the issuance of these types of subscriptions that might be committed by employees of the data controller or by the beneficiaries.

Until the date of the investigation, the transport company did not request an endorsement from the National Supervisory Authority, prior to the introduction of the procedure for collecting copies of ID cards, as required by Decision no. 132/2011 and the proof of consent of the data subjects or a legislative act allowing collection of copies of ID cards was not made.

As such, the data controller has been sanctioned for the offense provided for in Article 31 of Law no.677/2001, for incomplete notification, as the data controller, until the date of investigation, has not notified all personal data that they process in order to issue free or reduced rate subscriptions and the person entitled to such processing, contrary to the provisions of Article 22 of Law no. 677/2001, and for the offense prescribed by Article 32 of Law no. 677/2001, on the unlawful processing of personal data.

Also, following the investigation, it was ordered by decision to stop retaining copies of ID cards and the deletion of copies of identity cards already collected, when issuing and recharging reduced rate and free subscriptions.

The transport company informed the National Supervisory Authority that it has taken measures to comply with the decision and has stopped the retention of ID card copies, by pursuing computer deletion or destruction of the copies already collected.

CASE FILE (banking institutions)

Through the application lodged at the National Supervisory Authority, a petitioner has notified the retention of a copy of the identity card by a bank upon payment of monthly rate for a loan contracted by another person close to the petitioner, despite expressing his disagreement with this processing. The petitioner addressed the bank, but was not satisfied with the response.

After investigating a similar case in 2012, through a fact-finding / sanction report it was recommended that the said bank should adapt its internal procedures to Article 8 of Law no. 677/2001 and Decision no. 132/2011, concerning the situations in which it may be allowed to keep copies of ID cards; at that time, the bank was sanctioned for offenses provided in Article 32 of Law no. 677/2001, since it has retained, by collecting and storing, the personal identification number and series and number of the identity document, as well as other data contained in the identity document, by retaining the copy of the identity card of a complainant without his express consent, without having legal grounds or an endorsement from the National Supervisory Authority.

During the investigation conducted in 2013, the bank reiterated its previous reasoning by reference to the provisions of NBR Regulation no. 9/2008, according to which it is necessary for credit institutions to verify customer identity and preserve evidence of fulfilling this obligation, and to those of Law 656/2002, which requires banks to apply standard customer due diligence measures when there is suspicion that the transaction in question is money laundering or terrorist financing, if there are doubts about the veracity or relevance of the identification information previously obtained about the customer.

In the petitioner's case, he has completed a transaction to deposit cash into the account of another customer who had entered into a credit agreement with the bank, a contract to which the petitioner was a third party. For these reasons and because the complainant refused to submit a copy of the identity card, the bank has considered, in the application of the legal provisions invoked, that the transaction includes hints of suspicion and the standard customer due diligence measures should be applied to obtain identification information and documents of the customer.

On the other hand, regarding the measures taken to adapt banking practice to the incident legal provisions, following the recommendations of the National Supervisory

Authority in 2012, the bank said that it has modified its procedure of desk and cashier operations, which stipulates that "where the external depositor who deposits cash of up to 15,000 euro or other currency equivalent does not express his agreement to retain a copy of the identity document, the cashier will hand over Annex 7 Application for cash deposit to accounts opened with the bank to be completed. The cashier shall ensure the conformity of the particulars completed in the application of cash deposit with data from the external depositor's identity document. At the same time, it is provided that, for cash deposits worth more than 15,000 euro or other currency equivalent, it is compulsory to retain a copy of the identity document of the external depositor."

The bank addresses and the petition had not demonstrated that the petitioner fit the category of depositors for which it was mandatory to retain a copy of the identity card, and, therefore, being subject to the procedure changed by the bank in 2013. Therefore, in this situation, the retention of a copy of the identity card of the petitioner was not required.

Consequently, the data controller was again sanctioned for the offense provided and sanctioned under Article 32 of Law no. 677/2001, concerning the unlawful processing of personal data, as the bank had retained by collecting and storing the personal identification number and series and number of identity card, as well as the other data contained in the identity card, by retaining the copy of the identity document of the petitioner, without his express consent, in the absence of a legal basis or an endorsement from the National Supervisory Authority.

2. The transmission of commercial communications by electronic means

During the year 2013, the number of complaints and notices covering receipt of unsolicited commercial communications transmitted via telephone (calls or SMS) or e-mail has significantly increased, a number of 253 such petitions being registered. Most of them have touched on issues on the protection of privacy in the electronic communications sector from receiving unsolicited commercial electronic mail, without the recipient's express and unequivocal consent in this regard.

For the admissible complaints, the National Supervisory Authority conducted a series of investigations to determine whether the person sending the messages to the complainant had received consent to send such messages to the email address and if the complainant was offered with the possibility to oppose receiving more similar commercial messages in the

future. In some of the cases investigated, it was found that senders of commercial messages did not meet legal requirements in terms of obtaining prior consent, of ensuring a full informing regarding the identity and purpose, of the functioning of unsubscribe mechanism.

CASE FILE (on-line commercial transactions)

A complainant claimed that, after ordering a product via telephone from a particular company, he has subsequently begun to receive unsolicited commercial messages from the holder of another domain name. Following correspondence carried out via e-mail, he was informed by the company from which the product was ordered that an account was automatically created and that he was subscribed to the newsletter of the website from which he has started to receive unsolicited commercial messages, considering that the two shared the same communication platform. Following the petitioner's complaint, the customer's status in database was changed to "unsubscribed", without a certain date being available in which this operation was performed. Although it was reported that he was unsubscribed from the newsletter, the petitioner continued to receive unsolicited commercial messages. The company informed the complainant that, upon taking the telephone order, the account was erroneously saved on another domain that shares the same communication platform.

Representatives of the company argued that sending commercial communication is made with the consent of the customer, as potential customers (including the applicant) would be required to know the "Terms of Service" available on both sites, where it is stated that that personal data can be used to send information to the user about future promotions.

In the described situation, the consent given may not be considered as an expressly and freely expressed consent in advance by the recipient of commercial messages, for the precise and express purpose of receiving commercial communications, on the grounds of Article 12 of Law no. 506/2004; in the petitioner's case, the creation of the account was not performed directly and personally by him, and, furthermore, the explicit consent of the petitioner to receive commercial communications was not requested or obtained.

In regard to these findings, the data controller was sanctioned under Law no.677/2001 and Law no. 506/2004, since the company did not notify the National Supervisory Authority about the processing of data for purposes of advertising, marketing and publicity, the petitioner was sent unsolicited commercial communications by electronic mail, although he has not given his prior express consent to receive commercial communications by electronic

mail and that the company did not include in the first mails containing commercial content full information on the identity of the sender and a valid address where the applicant may request termination of commercial communications.

CASE FILE (tourism agencies)

A complainant complained about repeatedly receiving unsolicited commercial communications from a travel agency, claiming that he has never requested its services. The petitioner has also notified that commercial messages do not contain complete identification data of the travel agency that continued to send commercial messages after the date on which he has requested to stop receiving such messages by using the unsubscribe mechanism existing in the content of the messages.

From checking commercial messages received by the petitioner, it was found that they do not specify the exact name of a company. The National Supervisory Authority has taken steps to investigate several times, both in writing and by visiting the field office addresses available to the company. The representatives of the travel agency refused to provide the information requested by the National Supervisory Authority in the exercise of its investigative powers, while it was found that the commercial communications continued to be sent to the claimant, despite expressly manifesting his opposition to it in a repeated manner.

In regard to these findings, the data controller was sanctioned in accordance with Law no. 677/2001 and Law no. 506/2004, since the company has refused to provide information and to participate in the announced investigation, has repeatedly sent commercial communications by electronic mail to the petitioner, although he has not given his prior express consent to receive such commercial communications and it has not included in the majority of the messages sent complete information on the true identity of the sender.

3. Processing of personal data by means of video surveillance

In 2013, the number of complaints and notices covering the installation and operation of video surveillance systems that do not comply with the legal provisions and with Decision no. 52/2012 concerning the processing of personal data through the use of video surveillance, issued by the National Supervisory Authority, has increased. The target groups of data controllers are owners' associations and various entities in their quality of employers. Following the investigations performed in these cases, the most commonly

observed violations concerned the failure to notify the National Supervisory Authority prior to such processing, installation of surveillance means in the offices of employees without legal grounds and without the endorsement of our institution, as well as the failure to comply with the right to information on the delivery of all statements imposed by law and by Decision no. 52/2012.

CASE FILE (local public authorities)

Several complaints addressed to the National Supervisory Authority showed that, on the premises of a city hall, video surveillance cameras were installed, including all employee offices.

At the time of the investigation, it was found that in the town hall building two video surveillance systems were installed, one of which was installed in the two hallways and on the outside the building for purposes of monitoring / safety of people, premises and public / private assets and by which personal data is processed (the image).

Concerning the images taken from a number of eight offices in the city hall, through the second video surveillance system, these were not stored, and could only be viewed in real time.

Given that the city hall has not notified the National Supervisory Authority about the processing of personal data carried out by the video surveillance system, as required by Article 22 of Law no. 677/2001, and has not performed the complete information of the data subjects, as required by Article 12 of Law no. 677/2001, it was sanctioned in accordance with the provisions of Article 31 and Article 32 of Law no. 677/2001.

Following the investigation, the city hall decided to disable the video monitoring system installed in the office.

CASE FILE (owner associations)

In the petition addressed to the National Supervisory Authority, the petitioner informed that, during the year 2012, the homeowners association from where he resides installed a video surveillance system without consulting the members of the association in advance. It was also claimed that some cameras are mounted on the floor directly overlooking to the apartments without the consent of the owners. Also, the applicant stated that the homeowners association is not included in the register of personal data processing

for such processing.

Pursuant to the investigation, the homeowners association was sanctioned for committing the acts stated by Article 31 (failure to notify), Article 32 (failure to inform data subjects) and Article 33 (for lack of a procedure for the security of processing personal data) of Law 677/2001.

Following the inspection, the homeowners association decided to cease operation of the video surveillance system.

4. Reporting of personal data to credit bureau type filing systems

In 2013, the number of complaints aimed at the transmission of personal data to the credit bureau has diminished; however, investigations carried out in this area further revealed a number of issues regarding the type of information reported by banks and the manner and term of fulfilling the prior notification required by Law no. 677/2001 and Decision no. 105/2007 on the processing of personal data carried out in credit bureau type filing systems, demonstrating improper undertaking of these obligations by the respective data controllers.

CASE FILE

Through a petition registered at the National Supervisory Authority, several petitioners, members of the same family, have expressed dissatisfaction with the reporting of certain data concerning inconsistencies by a bank to the credit bureau.

Thus, the petitioners notified that they have requested a loan from the bank, one as borrower and others as co-payers and that, pursuant to their undertakings, they were informed by the bank (only) about the fact that this request was not approved. Subsequently, following a request from the petitioners to the Credit Bureau, they have found that the bank reported to the credit bureau data concerning errors, stating "document with inaccuracies, flawed documents".

Upon the petitioners' request to have their data referring to inaccuracies reported to the credit bureau deleted, since they were not informed in advance of this measure, according to the provisions of Decision no. 105/2007, the bank replied that it cannot resolve the request favourably and that their registration had been done in accordance with the provisions of this decision.

Pursuant to the investigation carried out with this data controller, it was found that the petitioners' data inaccuracies were sent to the credit bureau after more than 6 months after finding inconsistencies. Also, the bank did not provide adequate information to the petitioners, which would allow prior notice thereof within a reasonable time, to permit the building of an adequate defence before reporting data on the documents with inaccuracies to the credit bureau, considering the important impact that can be generated by such a report. In regard to the findings of the investigation, the data controller was fined for committing the offense of unlawful processing provided by Article 32 of Law no. 677/2001.

Also, the National Supervisory Authority issued a decision ordering the bank to delete the data inaccuracies, forwarded by it to the credit bureau.

Subsequently, the data controller has appealed in court against both the minutes fact-finding / sanction report, with the process being pending before the court, as well as against the decision of deletion issued by the National Supervisory Authority; the lawsuit was resolved in favour of the Authority.

CASE FILE

In the petition registered at the National Supervisory Authority, the petitioner expressed dissatisfaction with the reporting of negative data by a commercial bank to the credit bureau.

The complainant said that he concluded a credit agreement with a commercial bank, with the due date of each month being established on the 20th of each month. The petitioner further states that, upon the request of credit refinancing, he has found that negative data was reported on his name to the credit bureau, even though he was never late by more than 30 days with the payment of his monthly instalments. In addition, the applicant states that he was not informed 15 days before the reporting of negative data to the credit bureau.

The investigation carried out revealed that the applicant was erroneously reported to the credit bureau with a different amount than that owed. In this situation, the bank in question was punished for the offense provided for in Article 32 of Law no. 677/2001 for not abiding the provisions of this and those of Decision no. 105/2007.

Also, since prior information has not been made under these provisions, the bank was sanctioned for a violation under Article 32 of Law no. 677/2001. Following the investigation, the negative data that were incorrectly reported was deleted from the tracking system of the

Credit Bureau.

5. Disclosure of personal data to various entities

Through several complaints addressed to the National Supervisory Authority, legal issues relating to breach of the conditions under which personal data have been disclosed to third parties (employers, debt collection companies) were reported, without having obtained the consent of the data subject or without having given sufficient consideration of their right to information, where disclosure can be justified by the legitimate interests of the controller or the third party-recipient. Also, in some cases, it was found pursuant to the investigations carried that the disclosure of personal data was made without any legal basis or disproportionately to the aim pursued.

CASE FILE (service providers)

A complainant noticed a possible violation of the provisions of Law no. 677/2001 by a company providing internet and cable TV services, meaning that the latter illegally disclosed his personal information to a debt collection company.

Upon inspection, it was found that between the complainant and data controller there is a contractual relationship (remote commercial agreement, concluded as provided by Ordinance no. 130/2000).

The accused company claimed that its records indicated that the applicant had not handed over the equipment used in providing the service provided by the company, as well as the fact that debt collection is an amicable process that a provider of services to individual customers has implemented to ensure receipt of payment for the services rendered.

The alleged data controller invoked sending a type letter to the complainant in which it had informed him about the possibility of sending his data to a debt collection company. At the same time, it was found that the company providing Internet and cable TV services could not prove transmission of such letters to its customer and no proof of concluding a service agreement with him.

As such, the data controller has been sanctioned in accordance with the provisions of Article 32 of Law no. 677/2001, since the data controller has not provided evidence of informing the complainant in advance about the recipients to which its data was to be disclosed and, based on Article 33 of Law no. 677/2001, for breaching security measures

needed to be applied in respect of holding and archiving the agreement concluded with petitioner.

CASE FILE (banking institutions)

A petitioner has claimed that her right to privacy was violated by a bank as it has sent data about her account to her employer.

The complainant was informed beforehand by SMS and contacted by telephone several times on her personal and work number, as well as through notices of payment, concerning the arrears recorded for the monthly repayment of the contracted credit. Since the instalments were not paid on time, the bank decided to notify the employer of the complainant, citing, in this regard, the following clause in the loan agreement: "The Borrower and / or Joint Borrower irrevocably and unconditionally forward the Bank the right to receive all of his/their present and future income, including his/their salary / wages"; the bank said that it has requested support from the employer to help the petitioner to fulfil her payment obligations, mentioning in the notification sent to the employer that the complainant has assigned her income to the bank, empowering the bank in case of late payments to require the employer to withhold income amounts due monthly and to transfer them to the accounts specified by the bank.

On this occasion, by way of notification, the number and date of the credit agreement entered into by the petitioner, her IBAN account number, the amount due were disclosed to the employer. The bank sent a final warning message concerning the payment of arrears, stating that, if this will not be met, forced execution without further notice or notice of delay will be triggered. The employer did not comply with the request bank to transfer the amounts retained in the accounts given by it.

The Code of Civil Procedure provides that the enforcement procedures of an enforceable title, through the withholding of wages, can be carried out only at the stage of forced executions by judicial executors.

Banking law ensures privacy of data protected by bank secrecy, which includes the information related to late payments on a loan. Thus, Article 112 paragraph (2) of the Emergency Ordinance no. 99/2006 on credit institutions and capital adequacy provides that any person who performs administration and / or management responsibilities, or taking part in the activities of a credit institution is not entitled to use or disclose, either during or after

termination of the activity, facts or information which, if made public, would harm the interests or prestige of the credit institution or of any of its customers.

Processing of personal data must be made in good faith and in accordance with the laws in force in accordance with Article 4 paragraph (1) letter a) of Law no. 677/2001 and only with consent to the processing, expressly and unequivocally expressed (with the exceptions provided for in Article 5 paragraph (2) of Law no. 677/2001).

Or, the credit agreement used by the bank is a contract of adhesion, which, to the general manner in which the above clause was formulated at the date of investigation, does not allow free and unequivocal expression of consent by the borrowers for processing data in relation to third parties in various situations in which their data could be disclosed.

At the end of the investigation, the National Supervisory Authority decided to issue a recommendation to the bank, in order to amend the credit agreement by removing clauses that allow the bank to disclose personal information on the debtor to the employer or third parties, unless expressly provided by law or if the subjects have freely, expressly and unequivocally stated their consent to such processing operations. The National Authority for Consumer Protection was also notified on the possible existence of unfair clauses in the credit agreements of the bank.

The recommendations were undertaken by the bank.

6. Disclosure of personal data on the Internet

The National Supervisory Authority has registered a considerable number of complaints and notices regarding the disclosure of personal data on the Internet, either on pages belonging to public institutions or companies or by individuals on personal blogs or networks that enable transferring files between users. For complaints and notices deemed admissible, investigations were performed to resolve the issues raised, in all cases infringements being remedied shortly by data controllers, by deleting or making the information disclosed anonymous.

CASE FILE (central public authority)

A petitioner complained about the publishing on a public website of declarations of assets and interests belonging to her, in which the personal identification number and home address were visible. At the same time, the random checks of declarations of assets and

interests of other persons who hold public office in the institution, it was found that data was published on the full address of the declared real property or on the home address. In one of the declarations of assets and interests of the complainant, the personal identification number and home address were made to be anonymous. According to Article 6 paragraph (1) letter e) of the Law no. 176/2010 on integrity in the exercising of public dignities and functions, for amending and supplementing Law no. 144/2007 on the establishment, organization and functioning of the National Integrity Agency, as well as for amending and supplementing other laws, those responsible for implementing the provisions relating to declarations of assets and interests ensures the display and maintenance of these statements on the website of the institution, by making anonymous the address of the declared buildings, with the exception of the place where they are located, the address of the institution that manages the professional assets, of the personal identification number and the signature.

After the inspection carried out at the institution, its representatives stated that the declarations of assets and interests of the people within the organization who are required to submit these declarations are completed in two copies, one of them without personal data such as personal identification number and home address, in order to be later posted in this form on the Internet.

In the case of the petitioner's statement and of the other statements containing personal identification number, full address of the declared real property or home address, due to an error belonging to the person responsible within the public institution, that is tasked with displaying statements on the website, the personal data listed above were not anonymously posted on the Internet. During the investigation, personal data from the declarations of assets and interests mentioned above were made to be anonymous.

It was also found that the public institution did not have an internal procedure that describes the activities required to fulfil the service obligations resulting from completing declarations of assets and interests, blurring of personal data and their displaying on the Internet, according to the applicable legal provisions.

In regard to the findings, the accused data controller was sanctioned under Law no.677/2001, as the institution excessively processed personal data, by way of disclosure of personal data on the Internet consisting of personal identification number and home address or the address of the properties declared in the declarations of assets and interests of some people who have held or still hold public office. The data controller was fined for not having

taken sufficient appropriate technical and organizational measures in order to protect personal data against unauthorized disclosure.

CASE FILE (service providers)

A complainant complained about the publication by a data controller providing water supply services, in the local online press and on their personal website, of a list of debtors that contains surname, name, total outstanding invoice, city, street, number of outstanding invoices of several hundred people. Pursuant to the investigation in writing, the company said that data from the lists of debtors were used to achieve the legitimate interest of the data controller, of recovering the debts of the company, considering that this interest was not likely to prejudice the interests or the fundamental rights and freedoms of the data subjects.

The company did not release any other information to the Authority that would respond to other requests of the Authority (the way in which the informing of the data subjects was ensured concerning the disclosure, prior notifications sent to debtors, by attaching documentary evidence, how the claims concerning the rights provided by Law 677/2001 were resolved, the security and confidentiality measures of personal data processing, the notification submitted by the company for the processing of data belonging to the debtors) or evidence regarding the way in which it ensures of a fair balance between the interests of the data controller and the rights or interests of the data subjects.

In regard to these findings, the data controller was sanctioned in accordance with the provisions of Law no. 677/2001, since the company has discolsed, by publishing online, personal data of borrowers without making proof of prior direct informing of the debtors and without this processing being legitimate on the basis of legal provisions or other grounds that justify it and because it did not provide all the information required by the Authority.

Pursuant to the investigation, a decision was issued ordering the company to take steps to immediately delete all information identifying borrowers whose personal data have been published on its website. Following receipt of the decision, the company deleted the data from the site.

7. Failure to comply with the security and confidentiality measures referring to the processing of personal data

In 2013, the National Supervisory Authority was informed by some public institutions on the fact that security and privacy measures were breached on personal data collected by some data controllers through documents and contracts concluded (travel agency, public notary), as a result of negligence in the handling of documents or failure to adopt minimum security requirements to prevent unauthorized disclosure of personal data.

Following investigations, it was found that data controllers have taken technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, data collected by various documents prepared in conducting current business of data controllers, including copies of identity documents, passports, and driving licenses.

CASE FILE (travel agencies)

A police station notified the National Supervisory Authority in relation to a possible infringement of the provisions of Law no. 677/2001. In fact, the police station claimed that an individual has found, at the head of a bridge, several photocopies of identity documents, passports and driving licenses of persons from Timisoara County and neighbouring counties, documents stemming from a travel agency, then notifying the police station. The police station conducted research for the matter in question, taking statements from various people involved from the community.

Following investigations, it was found that one of the employees of the travel agency, acting as regional manager, decided to eliminate documents from the company's archive, papers which were no longer useful, this decision leading to taking a bag of such documents to his parents' home in order to destroy them by burning. From the statements of other persons involved, given at the police station, it was found that these documents were also handed to some neighbours to be destroyed, some of them reaching the head of a bridge where they were found.

At the time of the investigation, there were a series of procedures presented for the archiving and destruction of documents, for the security and control of computer systems that are used in the processing of personal data. The procedures mentioned were not dated and did not have a serial number from a register. Also, they did not comprise the annexes set in their contents, namely: archival lists, input-output registers of archived documents, minutes of scrapping and disposal from the archive of the documents with expired shelving time.

In fact, it was found that, at company level, document retention periods for collecting personal data were not established, there is no archival lists and no person delegated to deal with archiving. In addition, no conclusive evidence was presented regarding the training of employees with regard to the processing of personal data and their privacy.

Consequently, the data controller has been sanctioned for a violation provided and punished under Article 33, respectively, for failure to meet the obligations on the application of security and confidentiality measures in processing provided by Article 20, which aim to prevent the disclosure of ocuments containing personal data by unauthorized persons.

CASE FILE (public notaries)

The Ministry of Internal Affairs notified the National Supervisory Authority regarding disclosure on the Internet of several categories of personal data and has submitted, as evidence, an optical media containing stored document files with personal data. Through this notice, the National Supervisory Authority has been informed that on the Internet (ODC type network), notaries' documents were disclosed, representing several categories: addresses to other notaries, to central/local public authorities, powers of attorney, statements of individuals, statements of non-collaboration with the intelligence or of not belonging to the political police of certain magistrates within a prosecutor's office, authentications etc.

Pursuant to the investigation, the public notary who produced those documents recognized that these documents are real, they are edited on the computers of its employees, but has not explained how they came to be made public on the Internet. According to the notary, there were problems on these computers, resulting from infection with a computer virus.

At the time of the investigation, it was found that at the notary's office no internal procedures were adopted concerning the minimum security measures on processing personal data to be passed on the provisions of Order no. 52/2002 regarding the approval of minimum security requirements on the processing of personal data.

According to the findings, at the date of the investigation, access to the computers on which the notary edited documents was made without any authentication method. Also, the documents could be copied to external media and printed by anyone with access to the computer. Lack of authentication means that any person can access any personal data on any computer in the notary office and, as such, it was impossible to identify, in the logs, people

who had access to the computer equipment. It was also possible to copy any document on external storage media and, as a consequence, infection with viruses derived from the external storage media used.

The data controller was fined for the offense stipulated by Article 33 of Law no. 677/2001, since the data controller has not taken, until the investigation, sufficient privacy and security measures to protect personal data of customers, employees and collaborators (including special categories of data) against unauthorized access and disclosure, and against any other unlawful forms of processing, as required by Article 19 and Article 20 of Law no. 677/2001, which led to the online disclosure of their personal data.

CHAPTER V
INTERNATIONAL RELATIONS' ACTIVITIES

Considering the budgetary constraints existing in 2013, the National Supervisory Authority was unable to ensure representation to all the international events to which it was invited to participate.

Despite these limitations, the National Supervisory Authority had to fulfil a legal obligation to participate, as a member, to the meetings of supervisory bodies of Schengen, Europol, Eurodac, Customs, Visas — forums that bring together representatives of the national authorities for personal data protection from each EU country.

The topics discussed during these meetings have focused on issues referring to the capacity to exercise independent control of the national personal data protection, the right of access by data subjects, establishing supervisory powers of the joint control bodies.

This way, since Article 88 of the Treaty of Lisbon provides that Europol "will be governed by regulation," a Proposal for a Regulation of Europol, which will replace the provisions of Council Decision 2009/371 / JHA on the establishment of a European Police Office (Europol) - the current legal basis for the functioning of Europol was also under discussion in the Joint Supervisory Body of Europol.

The Proposal for a Europol Regulation has the following objectives:

■ Europol alignment with the requirements of the Lisbon Treaty, the adoption of a legal framework in accordance with the ordinary legislative procedure;

■ fulfilment of the Stockholm program objectives;

■ assignment of new responsibilities to Europol, taking over CEPOL tasks and establishing a legal basis for EU cybercrime centre;

■ ensuring high levels of data protection, in particular by enhancing supervisory duties;

■ improving Europol governance through increased efficiency and alignment with the principles set out in the Common Approach concerning decentralized agencies at EU level.

From the point of view of protecting personal data, the proposed regulation is of great importance, since the processing of information, including personal data is a primary reason for the existence of Europol.

The Stockholm Programme aims at further strengthening the area of freedom, security and justice, focusing on the interests and needs of citizens. It sets out the EU priorities in the field of justice and internal affairs for the period 2010 - 2014 and defines strategic legislative and operational guidelines in the area of freedom, security and justice, in accordance with Article 68 of the Treaty on European Union.

The Stockholm Programme Action Plan provides for certain measures which aim to ensure the protection of fundamental rights. These measures consist in strengthening the law on protection of personal data through a new comprehensive legal framework, as represented by the package consisting of the proposed Regulation of the European Parliament and of the Council on the protection of individuals with regard to personal data processing and the free movement of such data and the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the prevention, detection, investigation or prosecution of criminal offenses or the execution of sentences and the free movement of such data.

As in 2012, discussions on the proposed amendments to the legal framework on data protection at European level were another important element of the National Supervisory Authority's international activities.

The Proposal for a Regulation has achieved its goal of producing a text that reflects the growing importance of data protection in the EU legal order (based on Article 16 TFEU setting a new single legal basis for rules on data protection and Article 8 of the Charter of Fundamental Rights of the European Union). It maintains and reinforces basic principles of data protection and imposes clear and uniform obligations to data controllers, in order facilitate the free movement of personal data and provides a consolidated legal framework for

uniform application of laws by data protection authorities, whose powers were consolidated.

The rules proposed through the regulation will strengthen the rights of the data subjects and will place more responsibility on data controllers regarding how personal data is processed. Moreover, the role and powers of national supervisors are also strengthened.

The new legal framework should be consistent with other international agreements, including Convention 108 of the Council of Europe on the protection of individuals with regard to automatic processing of personal data and its Additional Protocol.

The modernization of the rules within the Council of Europe coincides with the legislative reform on the protection of personal data within the European Union. The review process will follow two main objectives, namely to meet the challenges to privacy as a result of the use of new communications technologies and to emphasize the importance of follow-up mechanisms on the implementation of the principles established by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981 (Convention 108).

A new data protection issue raised is the American electronic surveillance program PRISM allowing intelligence bodies in the United States to have access to data from abroad, including European states.

In this regard, information gathering is done directly from the servers of large providers in the USA. Thus, generally, e-mail, voice, image, information stored on an e-mail etc. can be collected. According to public sources, US secret service management mentioned that the data collected under this program are of a great value and are used to protect the United States against various types of threats. Unauthorized disclosure in connection with this program attracts significant risks to the security of American citizens.

There were also discussions on the subject of transmission of Passenger Name Record data (PNR) - the Agreement between Canada and the European Union on the transfer and processing of PNR data, as well as the dialogue with the Russian Federation on the exchange of PNR type data in terms of entry into force of a law with major impact on the activities of European air carriers, as well as the rights of EU citizens on the protection of personal data.

Given the increasingly frequent demands of third countries of transmitting Passenger Name Record data, as well as the use of these data for law enforcement purposes, the National Supervisory Authority considers it necessary to define a legal framework applicable to all future agreements on passenger data in order to avoid legal uncertainty for both airline data

controllers and Member States, as well as unnecessary administrative burdens caused by the need to comply with different sets of rules applicable to various third countries. At the same time, we note that any legal instrument on data transfer must fully meet the conditions laid down in the EU legal framework on the protection of personal data and privacy. We therefore need to ensure, at the same time, a system of protection of personal data which contains adequate rules and sufficient security guarantees to ensure an adequate level of protection of personal data.

As in previous years, given the technological developments, the agendas of the various subgroups attended by representatives of the Supervisory Authority addressed issues such as anonymization techniques—techniques used with the high volume of data generated by a variety of devices, networks; notification of security breaches—obligation imposed on data controllers in the telecommunications sector in accordance with the provisions of Directive 2002/58/EC; Impression devices—the use of combinations of non-unique characteristics of the Internet protocol or a combination of other information to identify a number of devices that may be present in the network, so that a person can be associated with said device and thus identified.

A forum for discussion of problematic issues facing data protection authorities in the current context is represented by the case handling workshops, whose agendas, in 2013, have included topics related to processing of personal data on the Internet and in particular the processing of minors' personal data within social networks.

One of the great challenges posed by global technological developments to the right to protection of personal data is the processing of these data in the context of profiling.

On this area of interest, the National Supervisory Authority participated in 2013, in the project funded by the European Commission on data protection and profiling, developed by UNICRI in collaboration with Amapola—Projects on Security and Safety of Cities Citizens, Technical University of Berlin, Institute for Law, Technology and Society of Tilburg and the Centre for European Policy in Romania. As a pilot authority, together with the data protection authorities in Germany, Italy, and the European Data Protection Authority, the National Supervisory Authority in Romania has submitted comments on the quality and relevance of the questions, the framing, the structure and complexity of the questionnaire used in the project. After this stage, the questionnaire was distributed to personal data protection authorities of the 27 EU member states and Switzerland.

One of the main objectives of the project is to collect and compare information and national practices on profiling to identify the risks posed by human rights profiling techniques. At the same time, the project focuses on identifying and addressing the challenges of technology to address the fundamental right to data protection. The results of this project will be made public in the year 2014.

CHAPTER VI
ACTIVITIES ON THE SUPERVISION OF PERSONAL DATA PROCESSING

In 2013, the National Supervisory Authority has resolved 8756 requests submitted by personal data controllers represented by notifications and applications requesting clarification of issues related to the processing of personal data carried out by them. In regard to the previous year, the analysis of the notification forms revealed the increasing complexity in terms of requests from data controllers.

Thus, a total of 7499 notifications regarding processing of personal data were solved, of which 6967 made on Romanian territory and 532 transfers of data to countries within the European Union, European Economic Area and third countries.

Of the 532 notifications to transfer data to entities abroad, 465 were declared transfers to countries in the European Economic Area and third countries with an adequate level of protection of the data recognized by the European Commission (including the United States, the entities that have joined the Safe Harbor principles), as well as transfers to third countries pursuant to Article 30 of Law no.677/2001, as modified and amended.

A number of 67 data transfers abroad on the basis of Article 29 paragraph (4) of Law no. 677/2001, as amended, were also declared by the data controllers to other data controllers and/or to data processors in third states on the basis of contracts with standard contractual clauses and after analyzing them a number of 36 authorisations for such transfers were issued.

At the same time, 1242 requests made by other data controllers on matters relating to the provisions of Law no. 677/2001, as amended, annual reports of public authorities and 24 points of view were issued. The latter points of view referred mainly to the following issues:

• the obligation to submit the notification, based on data processing exempted from notification under Law no. 677/2001 and the normative decisions issued by the Authority;

• the quality of data controller or data processor within a particular processing of personal data;

• the quality of data controller of individuals that install video surveillance systems for personal use;

• the quality of sub-contractors for data transfers based on Article 29 paragraph (4) of Law no. 677/2001, as modified and amended;

• determining the quality of data controller / data processor of authorized branches / local offices in Romania of entities from countries in the European Union, which notify the data transfers to third countries.

At the same time, the National Supervisory Authority has provided guidance to personal data controllers through its telephone dispatch system on a daily schedule and advising at its premises, providing information on the obligations and conditions under which personal data may be processed, in order to protect fundamental rights and freedoms of individuals.

Moreover, in order to clarify the conditions under which data controllers perform data processing notified to the Supervisory Authority, when there was a suspicion of circumstances in which data subjects' rights are infringed as well as a breach of the legal provision in this field, 23 ex officio investigations were proposed to be carried out.

Section 1 — The activity of registering personal data processing

Regarding data processing notified by the data controllers, on their own oath, in 2013, there was an increase in the number of data controllers in e-commerce, hotel and tourism services and advertising, marketing and publicity. Other notifications referred to data processing with purposes such as HR, selection and placement of workers, non-banking financial services such as pawn shops and currency exchange and monitoring / security of people, premises and / or public / private goods and spaces, through video surveillance.

Some entities that have notified the processing of personal data were associations and foundations, freelancers, associations of owners / tenants, to monitor people's access through cameras, entities providing financial and banking services to customers via vocal authentication, and other entities that perform monitoring and geographical localization of vehicles, which organize training and professional development courses or are engaged in

organizing exhibitions, conferences, symposia.

Depending on the specific activities that were the subject of data processing notified, the National Supervisory Authority advised the data controllers, in particular with regard to the provisions of Article. 4, Article 12, Article 19 and Article 20 of Law no. 677/2001, as amended. For example, the supervisory authority recommended them to collect from the data subjects only those particular data that are strictly necessary to achieve a specific, explicit and legitimate purpose, to obtain the express consent of the data subject, unless there are legal provisions governing the processing and to inform the data subjects on all the rights guaranteed to them by the Law no. 677/2001 and the concrete ways in which those rights may be exercised (which must be adequate in relation to the means used to process the data).

In order to further assist the data controllers, improvements were brought to the Guide on filling-in notification forms which is available on the Supervisory Authority's site, including specifying the situations where it is not necessary to notify, situations referred to within the decisions issued in this regard, namely Decision no. 90/2006, Decision no. 100/2007 and Decision no. 23/2012.

In this respect, it was found that associations and foundations primarily notified data processing performed following the performance of projects co-financed from European funds, within the Sectorial Operational Programme Development of Human Resources, Sectorial Operational Programme Competitiveness Enhancement Program 2007-2013. In order to guide data controllers that have notified such processing, a comprehensive guide on filling-in such notification forms (HRD Guide) is made available on the National Supervisory Authority's website site.

The data controllers that sell online products were recommended to collect only the data necessary to make deliveries online and, where appropriate, specific information in order to make direct marketing. Also, according to Decision no. 132/2011 of the President of the Authority on the conditions of processing the personal identification number and other personal data with a generally applicable identification function, it was recommended to this category of data controllers not to collect the personal identification number except in cases covered by a specific legal provision.

Associations of owners / tenants who have installed video surveillance equipment in building entrances were required to comply with the legal regulations, especially with regard to the legal obligation established under Article 12 paragraph (1) of Law no. 677/2001, as

modified and amended, as regulated by Article 11 of the Decision no. 52/2012. They were also warned that these bodies must bear in mind that the security measures adopted should include provisions which should clearly indicate that the access to/use of the video surveillance equipment is limited to persons which are clearly competent/authorised to do so and that such access/use is only performed in situations in which an incident has occurred and it involves the disclosure of footage to competent authorities (police, courts of law), in order to observe the tenants' right to private life.

Section 2 — The transfer of personal data abroad

Regarding data transfers abroad notified by data controllers, it was found that most did not require approval as it targeted the transmission of data to the countries within the European Economic Area and to countries for which the European Commission has recognized an adequate level of protection, as well as data transfers performed to third countries, as regulated by Article 30 of Law no. 677/2001, as amended. These activities focused on the areas of human resources, economic and financial management, selection and placement of labour and hotel and tourism services.

Also, transfers of data to third countries were notified under the provisions of Article 29 paragraph (4) of Law no. 677/2001, as amended, in accordance with the contracts entered into between the parties between which the data transfer occurs, according to the Decisions on standard contractual clauses for the transfer of personal data to data controllers or data processors, established in third countries, based on the provisions of Directive 95/46/EC of the European Parliament.

Transfers under contracts with standard clauses focused on activities in the following areas:

- Human resource management, creating a uniform database at group level;
- Economic and financial and administrative management;
- Hosting and data storage and provision of technical support services and telephone services;
- Conducting of clinical trials, pharmaco-vigilance incident reporting;
- Collecting data within the recruitment process;
- Optimization of the data management infrastructure;

- Remote IT "Service Desk" support to PC users within the company;

- Advertising and Public Relations (to entities in Serbia and the United States);

- Implementation and management of the system of warning / reporting violations ("whistleblowing") and transfer abroad of information collected under the 'whistleblowing' system (which allows employees to report suspicions of abuse, neglect or violations related to accounting issues, internal accounting controls or auditing, banking and financial crime).

In order to clarify the conditions in which the transfer of personal data to third countries is made, proposals were made to carry out investigations at the premises of the data controllers that have notified them and data controllers were asked, as appropriate, to address the deficiencies noticed during the investigations.

The National Supervisory Authority issued a total of 36 authorisations for transfers based on standard contractual clauses.

Besides data transfers performed under contracts with standard contractual clauses, the Supervisory Authority also received for analysis the documents submitted to similar authorities within the European Union in order to authorize transfers between members of a multinational company, based on binding corporate rules, as Romania is among those states that do not recognize such mutual transfers. These transfers are approved according to procedures established by the working documents adopted by the Article 29 Working Group of the European Commission, more precisely WP 108 and WP 133, for situations where the data exporter in the European Union and the data importer from a third country have the quality of data controllers, and WP 195 and WP 204, for situations where these entities have the capacity of data processors according to the provisions of Directive 95/46/EC.

Thus, the submissions were reviewed by the supervisory authorities in France, the Netherlands, Germany and the United Kingdom, following the authorization of transfers based on binding corporate rules and upon receipt the final document our institution will authorize transfers of personal data performed by entities in Romania, members of multinational companies.

Also, the Supervisory Authority has received from entities in Romania, as members of international corporations, the request to authorize transfers of data to third countries based on Binding Corporate Rules that are already approved by supervisors in countries of the European Union. They were informed about the legal procedure that must be met in order to receive authorization to data transfer towards members of their corporation, who are located

in European Union third countries.

CHAPTER VII
THE ECONOMIC MANAGEMENT OF THE AUTHORITY

For 2013, the National Supervisory Authority has had funds allocated through the State Budget Law no.5/2013, as amended and supplemented.

The final structure is as follows:

Lei

Indicator	Code	Initial Budget 2013	Updated Budget 31.12.2013	Expenses until 31.12.2013	Execution (%)
Total expenses	51.01	3.460.000	2.894.000	2.853.093	98,58
Staff expenses	10	2.529.000	2.333.000	2.324.408	99,63
Goods and services	20	912.000	544.000	527.897	97,03
Capital expenditure	71	19.000	17.000	16.299	95.87
Payments made in previous years				-15.511	

Existing restrictions on budget execution as a result of both negative budget amendment (-566,000 lei) imposed a permanent update of priorities to achieve the most important projects with the existing funds.

Thus, the final allocated budget, significantly decreased from the previous year, had the effect of resigning the procurement of goods and the diminishing of the number of ex officio investigations in the province.

Regarding the use of funds, we can specify the following:

The amount of personnel expenses of the National Supervisory Authority represented 80% of total funds allocated from the state budget, of which 2,324 thousand lei have been used effectively in loans. This amount is 194 thousand lei higher compared to 2012 (by occupying temporary positions through secondment); however, there is still a major shortage of staff (7 vacancies). Most staff costs related to payments made to the employment of employees in specialized departments.

Travel expenses represented 4.55% of total expenditure in 2013 compared to 4.3% in 2012, as a result of checks carried out in the country.

It should be noted that the National Supervisory Authority carries out its main functions through investigations and inspections at data controllers located on the territory of Romania, as well as diplomatic missions and consular offices of Romania in other states.

At EU level, the National Supervisory Authority has the obligation to participate in the Article 29 Working Group, in the working subgroups and those of the joint supervisory bodies (Schengen, Europol, Eurodac), as well as in the work carried out at the Council of Europe level. Expenditures for travel include these expenses.

The low levels of other expenditures on goods and services purchased, respectively 418,308 lei in 2013 as compared to 885,586 lei in 2012, is the result of several factors, among which the lowest price criterion applied in procurement, joined with the carefully determined technical requirements and budgetary restrictions and negative adjustments occurred during the third and fourth quarters.

The accounting policies used in preparing the annual financial statements are in accordance with valid accounting regulations. The financial situations give a fair picture of the reality of the financial position of the institution on compliance with the budget appropriation allocated to groups, headlines, articles and paragraphs of expenditure, as provided in the Authority's budget. The budgetary expenditures were made with the principles of legality, timeliness, continuity and efficiency.

As a conclusion on the management of allocated budgetary funds, we can indicate that they were used with maximum efficiency and based on a careful management conducted by our institution.